Training Program Catalog

NICE Specialty Areas

Table of Contents

Executive Cyber Leadership (EXL)

AWA 101 – Fundamentals of Application Security (30 mins)
AWA 102 – Secure Software Concepts (30 mins)
COD 102 – The Role of Software Security (10 mins)
COD 103 – Creating Software Security Requirements (10 mins)
COD 104 – Designing Secure Software (15 mins)
COD 105 – Secure Software Development (20 mins)
COD 106 – The Importance of Software Integration and Testing (15 mins)
COD 107 – Secure Software Deployment (10 mins)
COD 108 – Software Operations and Maintenance (10 mins)
DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)
DSO 201 – Fundamentals of Secure DevOps (30 mins)
TST 206 – ASVS Requirements for Developers (20 mins)

Exploitation Analysis (EXP)

DSO 211 – Identifying Threats to Containers in a DevSecOps Framework (20 mins)

Incident Response (CIR)

ENG 118 – Essential Incident Response (15 mins)

Knowledge Management (KMG)

DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)
DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)
ENG 110 – Essential Account Management Security (15 mins)
ENG 111 – Essential Session Management Security (15 mins)
ENG 112 – Essential Access Control for Mobile Devices (15 mins)
ENG 113 – Essential Secure Configuration Management (15 mins)
ENG 119 – Essential Security Audit & Accountability (15 mins)
ENG 121 – Essential Identification & Authentication (15 mins)
ENG 122 – Essential Physical & Environmental Protection (15 mins)
ENG 125 – Essential Data Protection (15 mins)
ENG 127 – Essential Media Protection (15 mins)

Legal Advice and Advocacy (LGA)

DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)
ENG 151 – Fundamentals of Privacy Protection (10 mins)
TST 206 – ASVS Requirements for Developers (20 mins)

Network Services (NET)

COD 252 – Securing Google Platform Applications & Data (COMING SOON) (25 mins)
COD 287 – Java Application Server Hardening (20 mins)
DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)
DES 210 – Hardening Linux/Unix Systems (30 mins)

DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)
DES 215 – Defending Infrastructure (UPDATED) (30 mins)
DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)
DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)
DSO 256 – DevSecOps in the Google Cloud Platform (COMING SOON) (20 mins)
SDT 323 – Improper Input Validation (10 mins)

Operate & Maintain (OM)

COD 141 – Fundamentals of Database Security (30 mins)
COD 252 – Securing Google Platform Applications & Data (COMING SOON) (25 mins)
COD 287 – Java Application Server Hardening (20 mins)
DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)
DES 210 – Hardening Linux/Unix Systems (30 mins)
DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)
DES 215 – Defending Infrastructure (UPDATED) (30 mins)
DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)
DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)
DSO 256 – DevSecOps in the Google Cloud Platform (COMING SOON) (20 mins)
DSO 303 – Automating Security Updates (20 mins)
DSO 305 – Automating CI/CD Pipeline Compliance (20 mins)
ENG 110 – Essential Account Management Security (15 mins)
ENG 111 – Essential Session Management Security (15 mins)
ENG 112 – Essential Access Control for Mobile Devices (15 mins)
ENG 113 – Essential Secure Configuration Management (15 mins)
ENG 119 – Essential Security Audit & Accountability (15 mins)
ENG 121 – Essential Identification & Authentication (15 mins)
ENG 122 – Essential Physical & Environmental Protection (15 mins)
ENG 125 – Essential Data Protection (15 mins)
ENG 127 – Essential Media Protection (15 mins)
SDT 323 – Improper Input Validation (10 mins)

Oversee & Govern (OV)

AWA 101 – Fundamentals of Application Security (30 mins)
AWA 102 – Secure Software Concepts (30 mins)
COD 102 – The Role of Software Security (10 mins)
COD 103 – Creating Software Security Requirements (10 mins)
COD 104 – Designing Secure Software (15 mins)
COD 105 – Secure Software Development (20 mins)
COD 106 – The Importance of Software Integration and Testing (15 mins)
COD 107 – Secure Software Deployment (10 mins)
COD 108 – Software Operations and Maintenance (10 mins)
DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)
DES 305 – Protecting Existing Blockchain Assets (20 mins)
DSO 201 – Fundamentals of Secure DevOps (30 mins)
DSO 205 – Securing the COTS Supply Chain (15 mins)
DSO 206 – Securing the Open Source Supply Chain (15 mins)
ENG 151 – Fundamentals of Privacy Protection (10 mins)
TST 206 – ASVS Requirements for Developers (20 mins)

Project Management/Acquisition and Program (PMA)

AWA 101 – Fundamentals of Application Security (30 mins)
AWA 102 – Secure Software Concepts (30 mins)
COD 102 – The Role of Software Security (10 mins)
COD 103 – Creating Software Security Requirements (10 mins)
COD 104 – Designing Secure Software (15 mins)
COD 105 – Secure Software Development (20 mins)
COD 106 – The Importance of Software Integration and Testing (15 mins)
COD 107 – Secure Software Deployment (10 mins)
COD 108 – Software Operations and Maintenance (10 mins)
DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)
DES 305 – Protecting Existing Blockchain Assets (20 mins)
DSO 201 – Fundamentals of Secure DevOps (30 mins)
DSO 205 – Securing the COTS Supply Chain (15 mins)
DSO 206 – Securing the Open Source Supply Chain (15 mins)
ENG 151 – Fundamentals of Privacy Protection (10 mins)
TST 206 – ASVS Requirements for Developers (20 mins)

Protect & Defend (PR)

ATK 201 – Using the MITRE ATT&CK Framework (15 mins)
DSO 301 – Orchestrating Secure System and Service Configuration (20 mins)
ENG 118 – Essential Incident Response (15 mins)
ENG 211 – How to Create Application Security Design Requirements (15 mins)
ENG 311 – Attack Surface Analysis & Reduction (25 mins)
TST 202 – Penetration Testing Fundamentals (25 mins)
TST 301 – Infrastructure Penetration Testing (45 mins)
TST 302 – Application Penetration Testing (45 mins)
TST 351 – Penetration Testing for TLS Vulnerabilities (12 mins)
TST 352 – Penetration Testing for Injection Vulnerabilities (12 mins)
TST 353 – Penetration Testing for SQL Injection (12 mins)
TST 354 – Penetration Testing for Memory Corruption Vulnerabilities (12 mins)
TST 355 – Penetration Testing for Authorization Vulnerabilities (12 mins)
TST 356 – Penetration Testing for Cross-Site Scripting (XSS) (12 mins)
TST 357 – Penetration Testing for Hardcoded Secrets (12 mins)
TST 358 – Penetration Testing Wireless Networks (12 mins)
TST 359 – Penetration Testing Network Infrastructure (12 mins)
TST 360 – Penetration Testing for Authentication Vulnerabilities (12 mins)

Risk Management (RSK)

COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)
DES 212 – Architecture Risk Analysis & Remediation (30 mins)
DES 222 – Applying OWASP 2017: Mitigating Injection (12 mins)
DES 223 – Applying OWASP 2017: Mitigating Broken Authentication (12 mins)
DES 224 – Applying OWASP 2017: Mitigating Sensitive Data Exposure (12 mins)
DES 225 – Applying OWASP 2017: Mitigating XML External Entities (12 mins)
DES 226 – Applying OWASP 2017: Mitigating Broken Access Control (12 mins)
DES 227 – Applying OWASP 2017: Mitigating Security Misconfiguration (12 mins)
DES 228 – Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (12 mins)
DES 229 – Applying OWASP 2017: Mitigating Insecure Deserialization (12 mins)
DES 230 – Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (12 mins)

DES 231 – Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (12 mins)
DES 271 – OWASP M1: Mitigating Improper Platform Usage (12 mins)
DES 272 – OWASP M2: Mitigating Insecure Data Storage (12 mins)
DES 273 – OWASP M3: Mitigating Insecure Communication (12 mins)
DES 274 – OWASP M4: Mitigating Insecure Authentication (12 mins)
DES 275 – OWASP M5: Mitigating Insufficient Cryptography (12 mins)
DES 276 – OWASP M6: Mitigating Insecure Authorization (12 mins)
DES 277 – OWASP M7: Mitigating Client Code Quality (12 mins)
DES 278 – OWASP M8: Mitigating Code Tampering (12 mins)
DES 279 – OWASP M9: Mitigating Reverse Engineering (12 mins)
DES 280 – OWASP M10: Mitigating Extraneous Functionality (12 mins)
DES 281 – OWASP IoT1: Mitigating Weak, Guessable or Hardcoded Passwords (12 mins)
DES 282 – OWASP IoT2: Mitigating Insecure Network Services (12 mins)
DES 283 – OWASP IoT3: Mitigating Insecure Ecosystem Interfaces (12 mins)
DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism (12 mins)
DES 285 – OWASP IoT5: Mitigating Use of Insecure or Outdated Components (12 mins)
DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection (12 mins)
DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage (12 mins)
DES 288 – OWASP IoT8: Mitigating Lack of Device Management (12 mins)
DES 289 – OWASP IoT9: Mitigating Insecure Default Settings (12 mins)
DES 290 – OWASP IoT10 Mitigating Lack of Physical Hardening (12 mins)
DES 312 – Protecting Cardholder Data (20 mins)
DSO 307 – Secure Secrets Management (20 mins)
ENG 114 – Essential Risk Assessment (15 mins)
ENG 150 – Meeting Confidentiality, Integrity, and Availability (30 mins)
ENG 251 – Risk Management Foundations (20 mins)
ENG 351 – Preparing the Risk Management Framework (20 mins)
ENG 352 – Categorizing Systems and Information within the RMF (10 mins)
ENG 353 – Selecting, Implementing and Assessing Controls within the RMF (20 mins)
ENG 354 – Authorizing and Monitoring System Controls within the RMF (20 mins)
TST 205 – Performing Vulnerability Scans (45 mins)

Securely Provision (SP)

COD 110 – Fundamentals of Secure Mobile Development (45 mins)
COD 152 – Fundamentals of Secure Cloud Development (20 mins)
COD 160 -Fundamentals of Secure Embedded Software Development (45 mins)
COD 170 – Identifying Threats to Mainframe COBOL Applications & Data (20 mins)
COD 201 – Secure C Encrypted Network Communications (15 mins)
COD 202 – Secure C Runtime Protection (15 mins)
COD 206 – Creating Secure C++ Code (15 mins)
COD 207 – Communication Security in C++ (15 mins)
COD 214 – Creating Secure GO Applications (30 mins)
COD 216 – Leveraging .NET Framework Code Access Security (CAS) (30 mins)
COD 217 – Mitigating .NET Security Threats (45 mins)
COD 219 – Creating Secure Code: SAP ABAP Foundations (90 mins)
COD 241 – Creating Secure Oracle DB Applications (45 mins)
COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)
COD 246 – PCI DSS 3: Protecting Stored Cardholder Data (15 mins)
COD 247 – PCI DSS 4: Encrypting Transmission of Cardholder Data (15 mins)
COD 248 – PCI DSS 6: Develop and Maintain Secure Systems and Applications (15 mins)
COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)
COD 251 – Defending AJAX-Enabled Web Applications (25 mins)

COD 253 – Creating Secure AWS Cloud Applications (45 mins)
COD 254 – Creating Secure Azure Applications (45 mins)
COD 255 – Creating Secure Code: Web API Foundations (20 mins)
COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)
COD 257 – Creating Secure Python Web Applications (45 mins)
COD 258 – Creating Secure PHP Web Applications (30 mins)
COD 259 – Node.js Threats & Vulnerabilities (30 mins)
COD 261 – Threats to Scripts (30 mins)
COD 262 – Fundamentals of Shell and Interpreted Language Security (30 mins)
COD 263 – Secure Bash Scripting (15 mins)
COD 264 – Secure Perl Scripting (15 mins)
COD 265 – Secure Python Scripting (15 mins)
COD 266 – Secure Ruby Scripting (15 mins)
COD 267 – Securing Python Microservices (30 mins)
COD 270 – Creating Secure COBOL & Mainframe Applications (25 mins)
COD 281 – Java Security Model (20 mins)
COD 283 – Java Cryptography (45 mins)
COD 284 – Secure Java Coding (30 mins)
COD 285 – Developing Secure Angular Applications (30 mins)
COD 286 – Creating Secure React User Interfaces (10 mins)
COD 301 – Secure C Buffer Overflow Mitigations (45 mins)
COD 302 -Secure C Memory Management (20 mins)
COD 303 – Common C Vulnerabilities & Attacks (20 mins)
COD 307 – Protecting Data in C++ (25 mins)
COD 308 – Common ASP.NET MVC Vulnerabilities and Attacks (45 mins)
COD 309 – Securing ASP.NET MVC Applications (30 mins)
COD 315 – Preventing Vulnerabilities in iOS Code in Swift (20 mins)
COD 316 – Creating Secure iOS Code in Objective C (30 mins)
COD 317 – Protecting Data on iOS in Swift (20 mins)
COD 318 – Protecting Data on Android in Java (20 mins)
COD 319 – Preventing Vulnerabilities in Android Code in Java (20 mins)
COD 321 – Protecting C# from Integer Overflows & Canonicalization (30 mins)
COD 322 – Protecting C# from SQL Injection (8 mins)
COD 323 – Using Encryption with C# (20 mins)
COD 324 – Protecting C# from XML Injection (8 mins)
COD 352 – Creating Secure JavaScript and jQuery Code (45 mins)
COD 361 – HTML5 Secure Threats (15 mins)
COD 362 – HTML5 Built in Security Features (20 mins)
COD 363- Securing HTML5 Data (20 mins)
COD 364 – Securing HTML5 Connectivity (20 mins)
COD 366 – Creating Secure Kotlin Applications (20 mins)
COD 370- Testing for OWASP 2017: Injection (15 mins)
COD 371 – Testing for OWASP 2017: Broken Authentication (12 mins)
COD 372 – Testing for OWASP 2017: Sensitive Data Exposure (12 mins)
COD 373 – Testing for OWASP 2017: XML External Entities (10 mins)
COD 374 – Testing for OWASP 2017: Broken Access Control (10 mins)
COD 375 – Testing for OWASP 2017: Security Misconfiguration (10 mins)
COD 376 – Testing for OWASP 2017: Cross Site Scripting (XSS) (15 mins)
COD 377 – Testing for OWASP 2017: Insecure Deserialization (10 mins)
COD 378 – Testing for OWASP 2017: Use of Components with Known Vulnerabilities (10 mins)
COD 379 – Testing for OWASP 2017: Insufficient Logging & Monitoring (10 mins)
COD 380 – Preventing SQL Injection in Java (8 mins)
COD 381 – Preventing Path Traversal Attacks in Java (8 mins)

COD 382 – Protecting Data in Java (30 mins)
COD 383 – Protecting Java Backend Services (30 mins)
COD 384 – Protecting Java from Information Disclosure (8 mins)
COD 385 – Preventing Race Conditions in Java Code (8 mins)
COD 386 – Preventing Integer Overflows in Java Code (8 mins)
CYB 301 – Fundamentals of Ethical Hacking (15 mins)
DES 101 – Fundamentals of Secure Architecture (20 mins)
DES 202 – Cryptographic Suite Services: Encoding, Encrypting & Hashing (45 mins)
DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)
DES 204 – Role of Cryptography in Application Development (15 mins)
DES 205 – Message Integrity Cryptographic Functions (45 mins)
DES 212 – Architecture Risk Analysis & Remediation (30 mins)
DES 222 – Applying OWASP 2017: Mitigating Injection (12 mins)
DES 223 – Applying OWASP 2017: Mitigating Broken Authentication (12 mins)
DES 224 – Applying OWASP 2017: Mitigating Sensitive Data Exposure (12 mins)
DES 225 – Applying OWASP 2017: Mitigating XML External Entities (12 mins)
DES 226 – Applying OWASP 2017: Mitigating Broken Access Control (12 mins)
DES 227 – Applying OWASP 2017: Mitigating Security Misconfiguration (12 mins)
DES 228 – Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (12 mins)
DES 229 – Applying OWASP 2017: Mitigating Insecure Deserialization (12 mins)
DES 230 – Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (12 mins)
DES 231 – Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (12 mins)
DES 255 – Securing the IoT Update Process (30 mins)
DES 260 – Fundamentals of IoT Architecture & Design (30 mins)
DES 271 – OWASP M1: Mitigating Improper Platform Usage (12 mins)
DES 272 – OWASP M2: Mitigating Insecure Data Storage (12 mins)
DES 273 – OWASP M3: Mitigating Insecure Communication (12 mins)
DES 274 – OWASP M4: Mitigating Insecure Authentication (12 mins)
DES 275 – OWASP M5: Mitigating Insufficient Cryptography (12 mins)
DES 276 – OWASP M6: Mitigating Insecure Authorization (12 mins)
DES 277 – OWASP M7: Mitigating Client Code Quality (12 mins)
DES 278 – OWASP M8: Mitigating Code Tampering (12 mins)
DES 279 – OWASP M9: Mitigating Reverse Engineering (12 mins)
DES 280 – OWASP M10: Mitigating Extraneous Functionality (12 mins)
DES 281 – OWASP IoT1: Mitigating Weak, Guessable or Hardcoded Passwords (12 mins)
DES 282 – OWASP IoT2: Mitigating Insecure Network Services (12 mins)
DES 283 – OWASP IoT3: Mitigating Insecure Ecosystem Interfaces (12 mins)
DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism (12 mins)
DES 285 – OWASP IoT5: Mitigating Use of Insecure or Outdated Components (12 mins)
DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection (12 mins)
DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage (12 mins)
DES 288 – OWASP IoT8: Mitigating Lack of Device Management (12 mins)
DES 289 – OWASP IoT9: Mitigating Insecure Default Settings (12 mins)
DES 290 – OWASP IoT10 Mitigating Lack of Physical Hardening (12 mins)
DES 306 – Creating a Secure Blockchain Network (20 mins)
DES 311 – Creating Secure Application Architecture (45 mins)
DES 312 – Protecting Cardholder Data (20 mins)
DSO 253 – DevSecOps in the AWS Cloud (20 mins)
DSO 254 – DevSecOps in the Azure Cloud (20 mins)
DSO 256 – DevSecOps in the Google Cloud Platform (COMING SOON) (20 mins)
DSO 302- Automated Security Testing (20 mins)
DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)
DSO 306 – Implementing Infrastructure as Code (20 mins)

DSO 307 – Secure Secrets Management (20 mins)
ENG 114 – Essential Risk Assessment (15 mins)
ENG 115 – Essential System & Information Integrity (15 mins)
ENG 116 – Essential Security Planning Policy & Procedures (15 mins)
ENG 117 – Essential Information Security Program Planning (15 mins)
ENG 120 – Essential Security Assessment & Authorization (15 mins)
ENG 123 – Essential Security Engineering Principles (15 mins)
ENG 124 – Essential Application Protection (15 mins)
ENG 126 – Essential Security Maintenance Policies (15 mins)
ENG 150 – Meeting Confidentiality, Integrity, and Availability (30 mins)
ENG 191 – Introduction to the Microsoft SDL (25 mins)
ENG 192- Implementing the Agile Microsoft SDL (20 mins)
ENG 193 – Implementing the Microsoft SDL Optimization Model (12 mins)
ENG 194 – Implementing Microsoft SDL Line of Business (20 mins)
ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)
ENG 205 – Fundamentals of Threat Modeling (45 mins)
ENG 212 – Implementing Secure Software Operations (20 mins)
ENG 251 – Risk Management Foundations (20 mins)
ENG 312 – How to Perform a Security Code Review (30 mins)
ENG 351 – Preparing the Risk Management Framework (20 mins)
ENG 352 – Categorizing Systems and Information within the RMF (10 mins)
ENG 353 – Selecting, Implementing and Assessing Controls within the RMF (20 mins)
ENG 354 – Authorizing and Monitoring System Controls within the RMF (20 mins)
SDT 311 – Testing for Integer Overflow or Wraparound (15 mins)
SDT 312 – Testing for (Path Traversal) Improper Limitation of a Pathname to a Restricted Directory (15 mins)
SDT 313 – Testing for (CSRF) Cross Site Request Forgery (15 mins)
SDT 314 – Testing for Unrestricted Upload of File with Dangerous Type (15 mins)
SDT 315 – Testing for Incorrect Permission Assignment for Critical Resource (15 mins)
SDT 316- Testing for Use of Hard-Coded Credentials (15 mins)
SDT 317 – Testing for Improper Control of Generation of Code (10 mins)
SDT 318 – Testing for Insufficiently Protected Credentials (10 mins)
SDT 319 – Testing for Out-of-bounds Read (10 mins)
SDT 320 – Testing for Out-of-bounds Write (10 mins)
SDT 321 – Testing for Uncontrolled Resource Consumption (10 mins)
SDT 322 – Testing for Improper Privilege Management (10 mins)
SDT 324 – Testing for Improper Restriction of Operations within the Bounds of a Memory Buffer (10 mins)
SDT 325 – Testing for NULL Pointer Dereference (10 mins)
SDT 326 – Testing for Use After Free (10 mins)
TST 101 – Fundamentals of Security Testing (20 mins)
TST 205 – Performing Vulnerability Scans (45 mins)

Software Development (DEV)

COD 110 – Fundamentals of Secure Mobile Development (45 mins)
COD 152 – Fundamentals of Secure Cloud Development (20 mins)
COD 160 -Fundamentals of Secure Embedded Software Development (45 mins)
COD 170 – Identifying Threats to Mainframe COBOL Applications & Data (20 mins)
COD 201 – Secure C Encrypted Network Communications (15 mins)
COD 202 – Secure C Runtime Protection (15 mins)
COD 206 – Creating Secure C++ Code (15 mins)
COD 207 – Communication Security in C++ (15 mins)
COD 214 – Creating Secure GO Applications (30 mins)
COD 216 – Leveraging .NET Framework Code Access Security (CAS) (30 mins)

COD 217 – Mitigating .NET Security Threats (45 mins)
COD 219 – Creating Secure Code: SAP ABAP Foundations (90 mins)
COD 241 – Creating Secure Oracle DB Applications (45 mins)
COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)
COD 246 – PCI DSS 3: Protecting Stored Cardholder Data (15 mins)
COD 247 – PCI DSS 4: Encrypting Transmission of Cardholder Data (15 mins)
COD 248 – PCI DSS 6: Develop and Maintain Secure Systems and Applications (15 mins)
COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)
COD 251 – Defending AJAX-Enabled Web Applications (25 mins)
COD 253 – Creating Secure AWS Cloud Applications (45 mins)
COD 254 – Creating Secure Azure Applications (45 mins)
COD 255 – Creating Secure Code: Web API Foundations (20 mins)
COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)
COD 257 – Creating Secure Python Web Applications (45 mins)
COD 258 – Creating Secure PHP Web Applications (30 mins)
COD 259 – Node.js Threats & Vulnerabilities (30 mins)
COD 261 – Threats to Scripts (30 mins)
COD 262 – Fundamentals of Shell and Interpreted Language Security (30 mins)
COD 263 – Secure Bash Scripting (15 mins)
COD 264 – Secure Perl Scripting (15 mins)
COD 265 – Secure Python Scripting (15 mins)
COD 266 – Secure Ruby Scripting (15 mins)
COD 267 – Securing Python Microservices (30 mins)
COD 270 – Creating Secure COBOL & Mainframe Applications (25 mins)
COD 281 – Java Security Model (20 mins)
COD 283 – Java Cryptography (45 mins)
COD 284 – Secure Java Coding (30 mins)
COD 285 – Developing Secure Angular Applications (30 mins)
COD 286 – Creating Secure React User Interfaces (10 mins)
COD 301 – Secure C Buffer Overflow Mitigations (45 mins)
COD 302 -Secure C Memory Management (20 mins)
COD 303 – Common C Vulnerabilities & Attacks (20 mins)
COD 307 – Protecting Data in C++ (25 mins)
COD 308 – Common ASP.NET MVC Vulnerabilities and Attacks (45 mins)
COD 309 – Securing ASP.NET MVC Applications (30 mins)
COD 315 – Preventing Vulnerabilities in iOS Code in Swift (20 mins)
COD 316 – Creating Secure iOS Code in Objective C (30 mins)
COD 317 – Protecting Data on iOS in Swift (20 mins)
COD 318 – Protecting Data on Android in Java (20 mins)
COD 319 – Preventing Vulnerabilities in Android Code in Java (20 mins)
COD 321 – Protecting C# from Integer Overflows & Canonicalization (30 mins)
COD 322 – Protecting C# from SQL Injection (8 mins)
COD 323 – Using Encryption with C# (20 mins)
COD 324 – Protecting C# from XML Injection (8 mins)
COD 352 – Creating Secure JavaScript and jQuery Code (45 mins)
COD 361 – HTML5 Secure Threats (15 mins)
COD 362 – HTML5 Built in Security Features (20 mins)
COD 363- Securing HTML5 Data (20 mins)
COD 364 – Securing HTML5 Connectivity (20 mins)
COD 366 – Creating Secure Kotlin Applications (20 mins)
COD 370- Testing for OWASP 2017: Injection (15 mins)
COD 371 – Testing for OWASP 2017: Broken Authentication (12 mins)
COD 372 – Testing for OWASP 2017: Sensitive Data Exposure (12 mins)

COD 373 – Testing for OWASP 2017: XML External Entities (10 mins)
COD 374 – Testing for OWASP 2017: Broken Access Control (10 mins)
COD 375 – Testing for OWASP 2017: Security Misconfiguration (10 mins)
COD 376 – Testing for OWASP 2017: Cross Site Scripting (XSS) (15 mins)
COD 377 – Testing for OWASP 2017: Insecure Deserialization (10 mins)
COD 378 – Testing for OWASP 2017: Use of Components with Known Vulnerabilities (10 mins)
COD 379 – Testing for OWASP 2017: Insufficient Logging & Monitoring (10 mins)
COD 380 – Preventing SQL Injection in Java (8 mins)
COD 381 – Preventing Path Traversal Attacks in Java (8 mins)
COD 382 – Protecting Data in Java (30 mins)
COD 383 – Protecting Java Backend Services (30 mins)
COD 384 – Protecting Java from Information Disclosure (8 mins)
COD 385 – Preventing Race Conditions in Java Code (8 mins)
COD 386 – Preventing Integer Overflows in Java Code (8 mins)
DES 202 – Cryptographic Suite Services: Encoding, Encrypting & Hashing (45 mins)
DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)
DES 204 – Role of Cryptography in Application Development (15 mins)
DES 205 – Message Integrity Cryptographic Functions (45 mins)
DES 212 – Architecture Risk Analysis & Remediation (30 mins)
DES 222 – Applying OWASP 2017: Mitigating Injection (12 mins)
DES 223 – Applying OWASP 2017: Mitigating Broken Authentication (12 mins)
DES 224 – Applying OWASP 2017: Mitigating Sensitive Data Exposure (12 mins)
DES 225 – Applying OWASP 2017: Mitigating XML External Entities (12 mins)
DES 226 – Applying OWASP 2017: Mitigating Broken Access Control (12 mins)
DES 227 – Applying OWASP 2017: Mitigating Security Misconfiguration (12 mins)
DES 228 – Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (12 mins)
DES 229 – Applying OWASP 2017: Mitigating Insecure Deserialization (12 mins)
DES 230 – Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (12 mins)
DES 231 – Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (12 mins)
DES 255 – Securing the IoT Update Process (30 mins)
DES 271 – OWASP M1: Mitigating Improper Platform Usage (12 mins)
DES 272 – OWASP M2: Mitigating Insecure Data Storage (12 mins)
DES 273 – OWASP M3: Mitigating Insecure Communication (12 mins)
DES 274 – OWASP M4: Mitigating Insecure Authentication (12 mins)
DES 275 – OWASP M5: Mitigating Insufficient Cryptography (12 mins)
DES 276 – OWASP M6: Mitigating Insecure Authorization (12 mins)
DES 277 – OWASP M7: Mitigating Client Code Quality (12 mins)
DES 278 – OWASP M8: Mitigating Code Tampering (12 mins)
DES 279 – OWASP M9: Mitigating Reverse Engineering (12 mins)
DES 280 – OWASP M10: Mitigating Extraneous Functionality (12 mins)
DES 281 – OWASP IoT1: Mitigating Weak, Guessable or Hardcoded Passwords (12 mins)
DES 282 – OWASP IoT2: Mitigating Insecure Network Services (12 mins)
DES 283 – OWASP IoT3: Mitigating Insecure Ecosystem Interfaces (12 mins)
DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism (12 mins)
DES 285 – OWASP IoT5: Mitigating Use of Insecure or Outdated Components (12 mins)
DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection (12 mins)
DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage (12 mins)
DES 288 – OWASP IoT8: Mitigating Lack of Device Management (12 mins)
DES 289 – OWASP IoT9: Mitigating Insecure Default Settings (12 mins)
DES 290 – OWASP IoT10 Mitigating Lack of Physical Hardening (12 mins)
DES 311 – Creating Secure Application Architecture (45 mins)
DSO 253 – DevSecOps in the AWS Cloud (20 mins)
DSO 254 – DevSecOps in the Azure Cloud (20 mins)

DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)
DSO 306 – Implementing Infrastructure as Code (20 mins)
ENG 123 – Essential Security Engineering Principles (15 mins)
ENG 124 – Essential Application Protection (15 mins)
ENG 191 – Introduction to the Microsoft SDL (25 mins)
ENG 192- Implementing the Agile Microsoft SDL (20 mins)
ENG 193 – Implementing the Microsoft SDL Optimization Model (12 mins)
ENG 194 – Implementing Microsoft SDL Line of Business (20 mins)
ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)
ENG 205 – Fundamentals of Threat Modeling (45 mins)
ENG 212 – Implementing Secure Software Operations (20 mins)
ENG 312 – How to Perform a Security Code Review (30 mins)
SDT 311 – Testing for Integer Overflow or Wraparound (15 mins)
SDT 312 – Testing for (Path Traversal) Improper Limitation of a Pathname to a Restricted Directory (15 mins)
SDT 313 – Testing for (CSRF) Cross Site Request Forgery (15 mins)
SDT 314 – Testing for Unrestricted Upload of File with Dangerous Type (15 mins)
SDT 315 – Testing for Incorrect Permission Assignment for Critical Resource (15 mins)
SDT 316- Testing for Use of Hard-Coded Credentials (15 mins)
SDT 317 – Testing for Improper Control of Generation of Code (10 mins)
SDT 318 – Testing for Insufficiently Protected Credentials (10 mins)
SDT 319 – Testing for Out-of-bounds Read (10 mins)
SDT 320 – Testing for Out-of-bounds Write (10 mins)
SDT 321 – Testing for Uncontrolled Resource Consumption (10 mins)
SDT 322 – Testing for Improper Privilege Management (10 mins)
SDT 324 – Testing for Improper Restriction of Operations within the Bounds of a Memory Buffer (10 mins)
SDT 325 – Testing for NULL Pointer Dereference (10 mins)
SDT 326 – Testing for Use After Free (10 mins)
TST 101 – Fundamentals of Security Testing (20 mins)

Systems Administration (ADM)

COD 141 – Fundamentals of Database Security (30 mins)
COD 252 – Securing Google Platform Applications & Data (COMING SOON) (25 mins)
COD 287 – Java Application Server Hardening (20 mins)
DES 210 – Hardening Linux/Unix Systems (30 mins)
DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)
DES 215 – Defending Infrastructure (UPDATED) (30 mins)
DSO 303 – Automating Security Updates (20 mins)
DSO 305 – Automating CI/CD Pipeline Compliance (20 mins)
ENG 110 – Essential Account Management Security (15 mins)
ENG 111 – Essential Session Management Security (15 mins)
ENG 112 – Essential Access Control for Mobile Devices (15 mins)
ENG 113 – Essential Secure Configuration Management (15 mins)
ENG 119 – Essential Security Audit & Accountability (15 mins)
ENG 121 – Essential Identification & Authentication (15 mins)
ENG 122 – Essential Physical & Environmental Protection (15 mins)
ENG 125 – Essential Data Protection (15 mins)
ENG 127 – Essential Media Protection (15 mins)
SDT 323 – Improper Input Validation (10 mins)

Systems Analysis (ANA)

COD 287 – Java Application Server Hardening (20 mins)
DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)
DES 210 – Hardening Linux/Unix Systems (30 mins)
DES 215 – Defending Infrastructure (UPDATED) (30 mins)
DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)
DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)
DSO 303 – Automating Security Updates (20 mins)
DSO 305 – Automating CI/CD Pipeline Compliance (20 mins)
ENG 110 – Essential Account Management Security (15 mins)
ENG 111 – Essential Session Management Security (15 mins)
ENG 112 – Essential Access Control for Mobile Devices (15 mins)
ENG 113 – Essential Secure Configuration Management (15 mins)
ENG 119 – Essential Security Audit & Accountability (15 mins)
ENG 121 – Essential Identification & Authentication (15 mins)
ENG 122 – Essential Physical & Environmental Protection (15 mins)
ENG 125 – Essential Data Protection (15 mins)
ENG 127 – Essential Media Protection (15 mins)

Systems Architecture (ARC)

COD 160 -Fundamentals of Secure Embedded Software Development (45 mins)
COD 201 – Secure C Encrypted Network Communications (15 mins)
COD 216 – Leveraging .NET Framework Code Access Security (CAS) (30 mins)
COD 217 – Mitigating .NET Security Threats (45 mins)
COD 241 – Creating Secure Oracle DB Applications (45 mins)
COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)
COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)
COD 257 – Creating Secure Python Web Applications (45 mins)
COD 258 – Creating Secure PHP Web Applications (30 mins)
COD 270 – Creating Secure COBOL & Mainframe Applications (25 mins)
COD 281 – Java Security Model (20 mins)
COD 283 – Java Cryptography (45 mins)
COD 285 – Developing Secure Angular Applications (30 mins)
COD 286 – Creating Secure React User Interfaces (10 mins)
COD 363- Securing HTML5 Data (20 mins)
COD 382 – Protecting Data in Java (30 mins)
COD 383 – Protecting Java Backend Services (30 mins)
DES 101 – Fundamentals of Secure Architecture (20 mins)
DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)
DES 204 – Role of Cryptography in Application Development (15 mins)
DES 205 – Message Integrity Cryptographic Functions (45 mins)
DES 212 – Architecture Risk Analysis & Remediation (30 mins)
DES 255 – Securing the IoT Update Process (30 mins)
DES 260 – Fundamentals of IoT Architecture & Design (30 mins)
DES 306 – Creating a Secure Blockchain Network (20 mins)
DES 311 – Creating Secure Application Architecture (45 mins)
DES 312 – Protecting Cardholder Data (20 mins)
DSO 302- Automated Security Testing (20 mins)
DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)

Systems Development (SYS)

COD 241 – Creating Secure Oracle DB Applications (45 mins)
COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)
COD 246 – PCI DSS 3: Protecting Stored Cardholder Data (15 mins)
COD 247 – PCI DSS 4: Encrypting Transmission of Cardholder Data (15 mins)
COD 248 – PCI DSS 6: Develop and Maintain Secure Systems and Applications (15 mins)
COD 251 – Defending AJAX-Enabled Web Applications (25 mins)
COD 253 – Creating Secure AWS Cloud Applications (45 mins)
COD 254 – Creating Secure Azure Applications (45 mins)
COD 255 – Creating Secure Code: Web API Foundations (20 mins)
COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)
COD 257 – Creating Secure Python Web Applications (45 mins)
COD 258 – Creating Secure PHP Web Applications (30 mins)
COD 259 – Node.js Threats & Vulnerabilities (30 mins)
COD 261 – Threats to Scripts (30 mins)
COD 262 – Fundamentals of Shell and Interpreted Language Security (30 mins)
COD 263 – Secure Bash Scripting (15 mins)
COD 264 – Secure Perl Scripting (15 mins)
COD 265 – Secure Python Scripting (15 mins)
COD 266 – Secure Ruby Scripting (15 mins)
COD 267 – Securing Python Microservices (30 mins)
COD 281 – Java Security Model (20 mins)
COD 283 – Java Cryptography (45 mins)
COD 284 – Secure Java Coding (30 mins)
COD 285 – Developing Secure Angular Applications (30 mins)
COD 286 – Creating Secure React User Interfaces (10 mins)
DES 202 – Cryptographic Suite Services: Encoding, Encrypting & Hashing (45 mins)
DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)
DES 204 – Role of Cryptography in Application Development (15 mins)
DES 205 – Message Integrity Cryptographic Functions (45 mins)
DES 255 – Securing the IoT Update Process (30 mins)
DES 311 – Creating Secure Application Architecture (45 mins)
DES 312 – Protecting Cardholder Data (20 mins)
DSO 253 – DevSecOps in the AWS Cloud (20 mins)
DSO 254 – DevSecOps in the Azure Cloud (20 mins)
DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)
DSO 306 – Implementing Infrastructure as Code (20 mins)
DSO 307 – Secure Secrets Management (20 mins)
ENG 115 – Essential System & Information Integrity (15 mins)
ENG 116 – Essential Security Planning Policy & Procedures (15 mins)
ENG 117 – Essential Information Security Program Planning (15 mins)
ENG 120 – Essential Security Assessment & Authorization (15 mins)
ENG 126 – Essential Security Maintenance Policies (15 mins)
ENG 212 – Implementing Secure Software Operations (20 mins)
ENG 312 – How to Perform a Security Code Review (30 mins)

Systems Requirements Planning (SRP)

COD 251 – Defending AJAX-Enabled Web Applications (25 mins)
COD 253 – Creating Secure AWS Cloud Applications (45 mins)
COD 254 – Creating Secure Azure Applications (45 mins)
COD 255 – Creating Secure Code: Web API Foundations (20 mins)
DES 101 – Fundamentals of Secure Architecture (20 mins)
DES 260 – Fundamentals of IoT Architecture & Design (30 mins)

DES 306 – Creating a Secure Blockchain Network (20 mins)
DSO 253 – DevSecOps in the AWS Cloud (20 mins)
DSO 254 – DevSecOps in the Azure Cloud (20 mins)
DSO 302- Automated Security Testing (20 mins)
DSO 306 – Implementing Infrastructure as Code (20 mins)
DSO 307 – Secure Secrets Management (20 mins)
ENG 114 – Essential Risk Assessment (15 mins)
ENG 115 – Essential System & Information Integrity (15 mins)
ENG 116 – Essential Security Planning Policy & Procedures (15 mins)
ENG 117 – Essential Information Security Program Planning (15 mins)
ENG 120 – Essential Security Assessment & Authorization (15 mins)
ENG 123 – Essential Security Engineering Principles (15 mins)
ENG 124 – Essential Application Protection (15 mins)
ENG 126 – Essential Security Maintenance Policies (15 mins)
ENG 191 – Introduction to the Microsoft SDL (25 mins)
ENG 192- Implementing the Agile Microsoft SDL (20 mins)
ENG 193 – Implementing the Microsoft SDL Optimization Model (12 mins)
ENG 194 – Implementing Microsoft SDL Line of Business (20 mins)
ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)
ENG 205 – Fundamentals of Threat Modeling (45 mins)
ENG 212 – Implementing Secure Software Operations (20 mins)
TST 101 – Fundamentals of Security Testing (20 mins)
TST 205 – Performing Vulnerability Scans (45 mins)

Targets (TGT)

DSO 211 – Identifying Threats to Containers in a DevSecOps Framework (20 mins)

Technology R&D (TRD)

DES 306 – Creating a Secure Blockchain Network (20 mins)

Test and Evaluation (TST)

COD 170 – Identifying Threats to Mainframe COBOL Applications & Data (20 mins)
COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)
COD 383 – Protecting Java Backend Services (30 mins)
CYB 301 – Fundamentals of Ethical Hacking (15 mins)
DSO 302- Automated Security Testing (20 mins)
ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)
ENG 205 – Fundamentals of Threat Modeling (45 mins)
TST 101 – Fundamentals of Security Testing (20 mins)
TST 205 – Performing Vulnerability Scans (45 mins)

Vulnerability Assessment and Management (VAM)

ATK 201 – Using the MITRE ATT&CK Framework (15 mins)
DSO 301 – Orchestrating Secure System and Service Configuration (20 mins)
ENG 211 – How to Create Application Security Design Requirements (15 mins)
ENG 311 – Attack Surface Analysis & Reduction (25 mins)
TST 202 – Penetration Testing Fundamentals (25 mins)

TST 301 – Infrastructure Penetration Testing (45 mins)
TST 302 – Application Penetration Testing (45 mins)
TST 351 – Penetration Testing for TLS Vulnerabilities (12 mins)
TST 352 – Penetration Testing for Injection Vulnerabilities (12 mins)
TST 353 – Penetration Testing for SQL Injection (12 mins)
TST 354 – Penetration Testing for Memory Corruption Vulnerabilities (12 mins)
TST 355 – Penetration Testing for Authorization Vulnerabilities (12 mins)
TST 356 – Penetration Testing for Cross-Site Scripting (XSS) (12 mins)
TST 357 – Penetration Testing for Hardcoded Secrets (12 mins)
TST 358 – Penetration Testing Wireless Networks (12 mins)
TST 359 – Penetration Testing Network Infrastructure (12 mins)
TST 360 – Penetration Testing for Authentication Vulnerabilities (12 mins)

All-Source Analysis (ASA)

DSO 211 – Identifying Threats to Containers in a DevSecOps Framework (20 mins)

Widespread adoption of cloud computing and DevOps have led to containers becoming the most popular and efficient way to deploy applications. However, containerization presents enterprise security risks that question existing security policies and compliance frameworks. This course provides a necessary understanding of known attacks required to improve the security of container application deployments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- The importance of Identifying threats to containers and data in the DevSecOps framework
- Why containers are particularly susceptible to image vulnerabilities, and how to mitigate the threat by rebuilding images as part of security updates.
- How to validate external images to prevent malware, unintended functionality, functional bugs, or components with known vulnerabilities into your environment
- Securely encrypting communication channels to avoid man-in-the-middle attacks designed to extract image contents, compromise credentials used to access registries or tamper with images being sent to orchestrators

Analyze (AN)

DSO 211 – Identifying Threats to Containers in a DevSecOps Framework (20 mins)

Widespread adoption of cloud computing and DevOps have led to containers becoming the most popular and efficient way to deploy applications. However, containerization presents enterprise security risks that question existing security policies and compliance frameworks. This course provides a necessary understanding of known attacks required to improve the security of container application deployments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- The importance of Identifying threats to containers and data in the DevSecOps framework
- Why containers are particularly susceptible to image vulnerabilities, and how to mitigate the threat by rebuilding images as part of security updates.
- How to validate external images to prevent malware, unintended functionality, functional bugs, or components with known vulnerabilities into your environment
- Securely encrypting communication channels to avoid man-in-the-middle attacks designed to extract image contents, compromise credentials used to access registries or tamper with images being sent to orchestrators

Customer Service and Technical Support (STS)

COD 141 – Fundamentals of Database Security (30 mins)

In practice, the database represents the goal of many attackers, as this is where the information of value is maintained. However, the functional requirements and security testing often focus on the interaction between a software user and the application, while the handling of data is assumed to be secure.

This course describes how to apply authentication and access control to your database and provides an understanding of database privileges and limiting data access. Coverage also includes techniques for protecting the database and methods for securely concealing specific data while providing an introduction to cloud databases and database encryption.

Cybersecurity Defense Infrastructure Support (INF)

DSO 301 – Orchestrating Secure System and Service Configuration (20 mins)

Building and maintaining quality software requires functional configuration management, but this is easier said than done in today's day and age. This process involves automation, but minimizing errors while securely and systematically managing changes in systems is complicated. This course provides Systems Developers, Network Operations Specialists, System Administrators, and Systems Security Analysts with the necessary skills to consistently and securely manage environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Identifying and mitigating gaps in your current orchestration security policies
- Ensuring the coordination and consistency of security policies across the enterprise
- The importance of maintaining immutability of live container instances, ensuring that changes occur in the source control and are only deployed via new versions of the resource
- Understanding the role of third-party tools such as Clair, Actuary, and Anchore in testing Infrastructure-as-Code (IAC) and Configuration-as-Code (CAC) platforms

---

ENG 118 – Essential Incident Response (15 mins)

This infrastructure security course teaches incident response policy development and the associated controls to help ensure appropriate communication and action throughout your organization.

Topics include:

- Incident response testing
- Incident handling
- Incident monitoring
- Incident reporting

ENG 211 – How to Create Application Security Design Requirements (15 mins)

To preserve the confidentiality, integrity, and availability of application data, software applications must be engineered with security in mind. Without defined security requirements, design choices will be made without security guidance and security testing cannot be effective.

This course provides technical and non-technical personnel with the knowledge to understand, create, and articulate security requirements as part of a software requirement document.

Topics include:

- Applying the application security maturity (ASM) model to the development process
- Key security engineering activities: gathering security objectives, applying security design guidelines, and creating threat models
- Identifying threats, attacks, vulnerabilities, and countermeasures
- How to conduct impactful security architecture and design reviews to identify potential security problems and minimize the application's attack surface.

ENG 311 – Attack Surface Analysis & Reduction (25 mins)

The attack surface of an application represents the number of entry points exposed to a potential attacker. The larger the attack surface, the larger the set of methods that can be used by an adversary breaking into software applications. Resultantly, minimizing it is a key exercise in risk reduction.

Topics covered:

- Understanding the goals and methodologies of attackers
- Identifying attack vectors that expose the application
- Defining and reducing an application's attack surface

TST 202 – Penetration Testing Fundamentals (25 mins)

Serving as a comprehensive way of testing for cybersecurity vulnerabilities Penetration Testing provides insight into a network, application, device, and/or physical security through the lens of an attacker to discover weaknesses and identify areas of improvement within your security posture. This course introduces concepts of penetration testing and provides an understanding of the stages of penetration testing as they relate to industry standards.

After completing this course, you will be able to:

- Conduct penetration testing according to an industry-standard methodology
- Identify the steps in a typical penetration testing process

---

TST 301 – Infrastructure Penetration Testing (45 mins)

Reliance on IT systems, regulatory compliance, and the evolving cyberthreat landscape are key indicators of the importance of Infrastructure penetration testing. Infrastructure Penetration tests can help inform cybersecurity strategies, validate existing security controls, and identify weaknesses in need of improvement. This course provides learners with the skills and knowledge necessary to perform penetration tests that simulate how attackers might attempt to compromise the organization's infrastructure.

After completing this course you will be able to:

- Perform pretest identification of potential vulnerabilities based on pretest analysis
- Leverage automated scanning tools
- Establish a baseline indication of the potential attack surface of the environment
- Interpret the results of automated tools to determine what additional testing is needed
- Perform host discovery, port scanning, and network segmentation checks
- Analyze the results of the penetration test are then compiled into a report

---

TST 302 – Application Penetration Testing (45 mins)

Applications store, process, and transmit data making them susceptible and vulnerable to hackers who can identify and exploit vulnerabilities. Penetration testing of these applications acts as a safeguard to reduce vulnerabilities and attack surface. This course provides learners with the skills and knowledge necessary to perform penetration tests that simulate how attackers might attempt to compromise the software applications.

After completing this course you will be able to:

- Conduct planning and reconnaissance
- Scan to understand how the target application will respond to various intrusion attempts
- Gain access using web application attacks, such as cross-site scripting, SQL injection, and backdoors, to uncover a target's vulnerabilities
- Maintain access to determine if the vulnerability can be used to achieve a persistent presence in the exploited system
- Analyze the results of the penetration test are then compiled into a report

---

TST 351 – Penetration Testing for TLS Vulnerabilities (12 mins)

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. However, flaws in TLS protocol include weak cryptographic primitives, or specific implementation errors, cross-protocol vulnerabilities, or any combination of each. This course teaches how to identify vulnerabilities, detecting acceptance of unencrypted connections, and testing configurations.

After completing this course, you will be able to:

- Identify typical TLS misconfiguration vulnerabilities
- Detect network services accepting unencrypted connections
- Test web server TLS configuration

TST 352 – Penetration Testing for Injection Vulnerabilities (12 mins)

Stemming from improperly sanitized or completely unsensitized input injection flaws allow attackers to relay malicious code through an application to another system. This course teaches how to identify and test for these vulnerabilities within your code.

After completing this course, you will be able to:

- Identify common injection vulnerabilities
- Test for command injection vulnerabilities
- Detect code and XML injection vulnerabilities
- Exploit command and code injection vulnerabilities

TST 353 – Penetration Testing for SQL Injection (12 mins)

Used to attack data-driven applications in which malicious SQL statements are inserted into an entry field for execution SQL Injection allows attackers to conduct a number of malicious activities to data including but not limited to becoming administrators of the database server. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Test for the presence of SQL Injection vulnerabilities
- Exploit SQL Injection vulnerabilities
- Identify the common tools and techniques used to exploit SQL Injection vulnerabilities

---

TST 354 – Penetration Testing for Memory Corruption Vulnerabilities (12 mins)

Occurring when the contents of a memory location are modified due to programmatic behavior that exceeds the intention of the original programmer or program/language constructs. This type of programming error can lead to a program crash or strange and bizarre program behavior. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Identify common memory corruption vulnerabilities
- Test for buffer overflows + Exploit known memory corruption vulnerabilities
- Understand advanced techniques for finding memory corruption vulnerabilities

---

TST 355 – Penetration Testing for Authorization Vulnerabilities (12 mins)

Authorization is the process of enforcing policies; determining what types of qualities of activities, resources, or services a user is permitted. Authorization vulnerabilities include forceful browsing and privilege escalation. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Identify common authorization vulnerabilities
- Test application access controls
- Exploit authorization vulnerabilities

TST 356 – Penetration Testing for Cross-Site Scripting (XSS) (12 mins)

Cross-site Scripting (XSS) is a client-side code injection attack where the attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Define the types of Cross-Site Scripting vulnerabilities
- Test applications for Cross-Site Scripting vulnerabilities
- Exploit Cross-Site Scripting vulnerabilities

TST 357 – Penetration Testing for Hardcoded Secrets (12 mins)

All modern applications rely on certain secrets to run from database connection strings to API keys or cryptographic keys. Keeping these secrets is critical to the security of the application as they typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This course teaches how to identify and test for the use of hard-coded credentials.

After completing this course, you will be able to:

- Determine whether an application contains hard-coded authentication credentials
- Determine whether an application contains hard-coded cryptographic keys
- Find plain-text secrets in application binaries
- Find leaked secrets in code repositories
- Identify techniques for advanced testing of application code for the presence of hard-coded secrets

---

TST 358 – Penetration Testing Wireless Networks (12 mins)

Wireless networks have security issues that are vulnerable to various attacks. Organizations need to proactively search out any weakness in security if they are to avoid unauthorized access to network resources and data leakage. This course introduces tools and techniques while teaching how to Identify and test for common attacks.

After completing this course, you will be able to:

- Test for the presence of unauthorized wireless networks
- Identify common attacks on wireless networks
- Identify the common tools and techniques for testing wireless networks

---

TST 359 – Penetration Testing Network Infrastructure (12 mins)

Essential to every organization; Infrastructure penetration testing provides an opportunity to know about the current situation of a company and analyze existing potential breach points. The process includes all internal computer systems, associated external devices, internet networking, cloud, and virtualization testing. This course teaches how to perform Network Infrastructure penetration tests, perform necessary scans, and test controls.

After completing this course, you will be able to:

- Perform network-layer penetration tests
- Test network segmentation controls
- Perform a network scan to discover active devices
- Perform a port scan on a host to identify exposed network services

---

TST 360 – Penetration Testing for Authentication Vulnerabilities (12 mins)

Building authentication and session management schemes correctly is a difficult task often presenting flaws that may equally difficult to Identify. Common authentication attacks consist of brute force, insufficient authentication, and weak password recovery validation. These types of attacks target and attempt to exploit the authentication process a web site uses to verify the identity of a user, service, or application. This course teaches how to execute attacks, identify vulnerabilities, and verify controls.

After completing this course, you will be able to:

- Identify common authentication vulnerabilities
- Verify authentication controls
- Execute dictionary attacks

Cybersecurity Management (MGT)

DES 305 – Protecting Existing Blockchain Assets (20 mins)

Blockchain implementation poses a number of challenges from storage capacity and scalability to anonymity and data privacy thus making the protection of existing assets complex. This course provides learners with an understanding of how to secure existing Blockchain assets against security threats.

After completing this course you will be able to:

- Secure the cryptographic keys that allow access to the ledger
- Use hardware security modules (HSMs)
- Ensure the integrity of “Smart Contracts”
- Protect communications between nodes

DSO 201 – Fundamentals of Secure DevOps (30 mins)

Building a culture of collaboration between software development (Dev) and information-technology operations (Ops) is full of challenges and learning. The notion of DevOps requires a good understanding of complex technical problems and business needs at the same time. This course introduces learners to the philosophy and provides the fundamental knowledge needed to execute practices that shorten system development lifecycles and provide continuous delivery with high software quality.

After completing this course you will be able to:

- Understand the unique opportunities for including security in your DevOps pipeline
- Understand at which points in your development process—from architecture to deployment—you can improve security
- Automate security compliance and controls using a variety of open-source tools
- Identify opportunities for increased collaboration and better feedback loops

---

DSO 205 – Securing the COTS Supply Chain (15 mins)

The usage of Commercial-off-the-shelf software (COTS) by organizations while advantageous comes with its own set of challenges and complexities. Unfortunately, it is rare for acquisition approaches to account for complex software supply chains; this course provides learners with an understanding of how to apply DevSecOps best practices to reduce software supply chain risks.

After completing this course you will be to:

- Employ acquisition strategies, contract tools, and procurement methods for the purchase of the software, COTS from suppliers
- Conduct a supplier review prior to entering into a contractual agreement to acquire the COTS
- Conduct an assessment of the COTS prior to selection, acceptance, or update
- Employ security safeguards to validate that the COTS received is genuine and has not been altered
- Establish and retains the unique identification of supply chain elements, processes, and actors for the COTS
- Establish a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements

---

DSO 206 – Securing the Open Source Supply Chain (15 mins)

As modern software development evolves, organizations are finding themselves leveraging Open Source Software to reduce costs, simplify operations, accelerate innovation, and improve interoperability. Adoption is expected to continue, but distribution and licenses allow anyone to use, view, modify, and share source code, which introduces new security vulnerability risks into the supply chain. This course provides learners with an understanding of how to apply DevSecOps best practices to reduce software supply chain risks inherent with the use of open-source software.

After completing this course you will be to meet compliance requirements while developing a DevSecOps mindset, including:

- Expanding the development teams use of dependency checking tools, including integration into the build process
- Ensuring application security teams implement security tests to audit select open-source software and components
- Establishing a build process that ensures the installation of the latest open software releases for operations teams migrating server platforms to containers
- Understanding the importance of monitoring repo feeds and CVEs, especially critical libraries such as OpenSSL that could affect many different products

---

ENG 151 – Fundamentals of Privacy Protection (10 mins)

Staying current on legislation and engaging the business on timely privacy compliance and practical solutions can be challenging. As the focus on compliance continues to increase, and the GRC landscape continues to evolve, compliance officers need to keep pace with emerging regulations. This course provides learners with a clear understanding of their role in meeting compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Enable better privacy engineering practices that support privacy by design concepts
- Ensure collaboration on privacy protection objectives across your organization
- Apply the NIST Privacy Framework to meet region-specific regulations such as GDPR and CCPA
- Communicate privacy practices with individuals, business partners, assessors, and regulators

---

Data Administration (DTA)

COD 141 – Fundamentals of Database Security (30 mins)

In practice, the database represents the goal of many attackers, as this is where the information of value is maintained. However, the functional requirements and security testing often focus on the interaction between a software user and the application, while the handling of data is assumed to be secure.

This course describes how to apply authentication and access control to your database and provides an understanding of database privileges and limiting data access. Coverage also includes techniques for protecting the database and methods for securely concealing specific data while providing an introduction to cloud databases and database encryption.

DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)

This course provides DevOps Engineers, IT Architects and Network Engineers responsible for the security of applications and data with the skills and knowledge required to protect their organization's cloud infrastructure.

Topics Include:

- The role of Data Encryption
- Identity and Authentication
- Firewalls and Network Security (SDNs, VPNs, DMZs)
- Division of Duties
- Compliance requirements
- Securing VM and Containers

DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)

Using Microservices, organizations can isolate software functionality into multiple independent modules that are individually responsible for performing precisely defined, standalone tasks communicating with each other through simple, universally accessible application programming interfaces (APIs). Containers enable developers to simultaneously build and ship these microservices; integrate them with other systems and automatically orchestrate them using predefined rules and processes.

This course is designed to educate DevOps Engineers, IT Architects, and Network Engineers working in Linux or on the cloud to add value to the application lifecycle through proper orchestration and enable faster development and fault-prone provisioning and configurations.

Topics Include:

- Hardening the OS
- Vulnerability Scanning
- Docker, SELinux and AWS Microservices
- API Gateways
- Node monitoring with Prometheus
- Implementing OAuth
- Schedulers and Orchestrators
- Defining a Pod Security Policy
- Using Metadata Concealment

Executive Cyber Leadership (EXL)

AWA 101 – Fundamentals of Application Security (30 mins)

This course introduces the fundamentals and primary drivers of application security.

Topics include:

- Core concepts of application security risk management
- Anatomy of an application attack
- Common attack scenarios juxtaposed with key security principles

- Best practices for developing secure applications

AWA 102 – Secure Software Concepts (30 mins)

This course provides a high-level overview of secure software concepts for web applications including application security, security standards, secure development methodologies, and security best practices.

Topics include:

- Current application security threat landscape
- Common security vulnerabilities
- Evaluating and mitigating the most common application security risks
- Security-related tasks for each stage in the software development lifecycle
- How to implement a security strategy based on your organization's risk

---

COD 102 – The Role of Software Security (10 mins)

This course introduces you to the overriding importance of software security for your organization, and the potential business consequences of developing and deploying insecure software.

Topics include:

- The difference between software security and network security
- Business imperatives for software security, including the high business costs of security breaches
- Compliance and legal implications of security breaches
- Customer expectations of security
- The increasing threat landscape

COD 103 – Creating Software Security Requirements (10 mins)

This course discusses the requirements phase of the software development lifecycle and provides software development teams with the knowledge and skill required to gather security requirements for the software that they are designing and implementing.

Topics Include:

- Identifying potential attacks and exploits
- Legal Security Requirements
- Business Requirements
- Customer Security Requirements

COD 104 – Designing Secure Software (15 mins)

This course provides learners with the skill and knowledge required to perform threat modeling, and ensure that security principles are applied at each step of the design process.

Topics Include:

- Integrating attack surface reduction
- Secure defaults
- Least privilege
- Defense in depth
- Compartmentalization

COD 105 – Secure Software Development (20 mins)

This course introduces you to secure development models, standards, and guidelines that provide you with a structure for reducing risk from application security vulnerabilities.

Topics Include:

- The role of Industry standards and security models like OWASP Top 10, CWE SANS Top 25, PA-DSS and many more

- The common criteria for Information Technology Security Education
- Formal methods applied to the analysis of software to ensure that it adheres to industry standards such as Code Analysis, Static Analysis, and Binary Analysis

---

COD 106 – The Importance of Software Integration and Testing (15 mins)

This course introduces you to the Integration and Testing phases of the software development lifecycle, including the roles of Code Review, Fault Injection, Vulnerability Scanning, Penetration Testing, and Static Analysis.

Topics Include:

- Pros and cons of performing a code review
- Resources available when conducting a code review
- Identifying vulnerabilities that may have been missed by other secure testing techniques
- Utilizing fault injection
- Vulnerability Scanning and Penetration Testing
- Pros and cons of static analysis

COD 107 – Secure Software Deployment (10 mins)

This course describes general principles to think about for improving your deployment process, best practices for logging and monitoring, as well as different ways to defend the operating system, web server and the database.

After complicating this course you will understand attack surface reduction, compartmentalization, defense in depth, least privilege deployment, secure defaults and security incident response plans.

COD 108 – Software Operations and Maintenance (10 mins)

This course covers best practices for logging and monitoring, as well as security misconfiguration and mitigation techniques.

After completing this course you will understand application security patching processes, strategies for defense-in-depth, and mechanisms to ensure sufficient logging and monitoring.

DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)

The PCI Secure SLC Standard outlines security requirements and assessment procedures for software vendors to validate how they properly manage the security of payment software throughout the entire software lifecycle. This course provides baseline knowledge needed to implement security requirements and assessment procedures to validate proper management of the security of payment software throughout the entire software lifecycle.

After completing this course you will be able to:

- Identify and mitigate common threats and vulnerabilities defined in the PCI Secure SLC standard
- Build an environment for secure software development, change control, and management
- Improve communications for secure deployment, configuration and software updates.

DSO 201 – Fundamentals of Secure DevOps (30 mins)

Building a culture of collaboration between software development (Dev) and information-technology operations (Ops) is full of challenges and learning. The notion of DevOps requires a good understanding of complex technical problems and business needs at the same time. This course introduces learners to the philosophy and provides the fundamental knowledge needed to execute practices that shorten system development lifecycles and provide continuous delivery with high software quality.

After completing this course you will be able to:

- Understand the unique opportunities for including security in your DevOps pipeline
- Understand at which points in your development process—from architecture to deployment—you can improve security
- Automate security compliance and controls using a variety of open-source tools

- Identify opportunities for increased collaboration and better feedback loops

---

TST 206 – ASVS Requirements for Developers (20 mins)

Ensuring developers understand application security needs can be overwhelming, but leveraging OWASP ASVS organizations can test and prove applications meet specific levels of security. This course is designed to equip Privacy and Cybersecurity Management with the knowledge required to provide development teams with a basis for testing web application technical security controls and a list of requirements for secure development in adherence to the Application Security Verification Standard (ASVS) 3.0 standard.

Upon successful completion of this course, learners will have the knowledge and skills required to meet ASVS compliance requirements, including:

- Using the ASVS to audit applications and to establish both internal and procurement metrics
- Understanding the role of ASVS Levels and Threat profiles
- Providing the necessary guidance and training to ensure your organization meets ASVS requirements.

Exploitation Analysis (EXP)

DSO 211 – Identifying Threats to Containers in a DevSecOps Framework (20 mins)

Widespread adoption of cloud computing and DevOps have led to containers becoming the most popular and efficient way to deploy applications. However, containerization presents enterprise security risks that question existing security policies and compliance frameworks. This course provides a necessary understanding of known attacks required to improve the security of container application deployments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- The importance of Identifying threats to containers and data in the DevSecOps framework
- Why containers are particularly susceptible to image vulnerabilities, and how to mitigate the threat by rebuilding images as part of security updates.
- How to validate external images to prevent malware, unintended functionality, functional bugs, or components with known vulnerabilities into your environment
- Securely encrypting communication channels to avoid man-in-the-middle attacks designed to extract image contents, compromise credentials used to access registries or tamper with images being sent to orchestrators

---

Incident Response (CIR)

ENG 118 – Essential Incident Response (15 mins)

This infrastructure security course teaches incident response policy development and the associated controls to help ensure appropriate communication and action throughout your organization.

Topics include:

- Incident response testing
- Incident handling
- Incident monitoring
- Incident reporting

Knowledge Management (KMG)

DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)

The adoption of cloud services involves various roles making it difficult to govern the selection and brokering of cloud services while adhering to policies and procedures. This course is designed to ensure privacy and security teams may effectively and efficiently adopt cloud computing in support of strategic and business goals.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Creating Policies, Procedures, Standards, and Controls that meet all regulatory and legal requirements, industry standards, and technical controls such as encryption.
- Establishing, deploy and assess a compliance baseline that determines targets
- Handling sensitive data, including how to identify and classify data, define data retention periods, and comply with data storage requirements.
- Prepare for compliance auditing and Reporting

DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)

This course is designed for Network Operations Specialists and aligns with the NICE requirements for the secure planning, implementation, and operation of network services and systems, including hardware and virtual environments.

Coverage includes:

- Security Principles
- Network Topologies
- Demilitarized Zones
- Routers, Switches, Bridges, and Firewalls
- Wireless Access Points
- Transmission Media
- Network Authentication
- Server Configuration

ENG 110 – Essential Account Management Security (15 mins)

This infrastructure security course provides essential guidance on implementing specific account management security controls at the hardware and software level to facilitate compliance with applicable regulatory requirements.

Topics include:

- How to define and control network access
- Creating a separation of duties policy
- Building and managing segregation of resources strategies
- Monitoring system access
- Using digital certificates for authentication

ENG 111 – Essential Session Management Security (15 mins)

This infrastructure security course provides guidance to system designers and developers on how to implement session management controls at the software level. These techniques enhance security of web applications and facilitates compliance with applicable regulatory requirements.

Topics include:

- Securing session identifiers
- Implementing Transport Layer Security (TLS) so sensitive data is always transmitted over secure channels
- Ensuring client browsers send cookies over HTTPS connections

---

ENG 112 – Essential Access Control for Mobile Devices (15 mins)

This infrastructure security course teaches designers and developers how to implement software-level access controls on mobile devices to mitigate threats, protect privacy, and comply with applicable regulatory requirements.

Topics include:

- Identifying threats to mobile devices
- The importance of protecting user privacy and confidentiality
- Methods for encrypting data at rest and data in transit
- Implementing application code signing to ensure software integrity

---

ENG 113 – Essential Secure Configuration Management (15 mins)

This infrastructure security course trains program managers, system designers, and developers on proper security practices for defining and implementing IT system configuration management.

Topics include:

- Key configuration practices and configuration change control
- Security impact analysis
- Access restrictions for change
- Principle of least functionality
- Information system component inventory

ENG 119 – Essential Security Audit & Accountability (15 mins)

This infrastructure security course trains information system owners, system administrators, and information system security officers on how to build and communicate effective audit policies and controls.

Topics include:

- Documenting security audits
- Implementing audit controls
- Using audit tools
- Generating audit reports

ENG 121 – Essential Identification & Authentication (15 mins)

This infrastructure security course teaches those responsible for information security how to develop identification and authentication policy and controls. The course spans personnel, devices, and information systems.

Topics include:

- Identification and authentication of users inside and outside your organization
- Device identification and authentication
- Identifier management
- Authenticator management and feedback
- Cryptographic module authentication
- Service identification and authentication
- Adaptive identification and authentication
- Processes for re-authentication

ENG 122 – Essential Physical & Environmental Protection (15 mins)

This infrastructure security course educates those responsible for developing physical and environmental protection policies how to create effective controls and comply with applicable regulatory requirements.

Topics include:

- Physical access authorizations and control
- Access control for transmission medium and output devices
- Monitoring physical access
- Information leakage, asset monitoring and tracking

ENG 125 – Essential Data Protection (15 mins)

This infrastructure security course delivers training to personnel in information systems, information security, systems design, software development, and IT operations on essential data security techniques. Focus is primarily on cryptographic controls at the information systems level and compliance with applicable regulatory requirements.

Topics include:

- Asymmetric key algorithms
- Using hash functions to protect data integrity
- Proper password storage for authentication purposes
- Encrypting file transfers and downloads
- Adding salt values before hashing
- Using Certificate Authorities

ENG 127 – Essential Media Protection (15 mins)

This infrastructure security course describes the development and dissemination of an organization-wide information media protection policy that addresses scope, roles, responsibilities, and coordination among organizational entities to facilitate compliance with applicable regulatory requirements.

Topics include:

- Best practices for media protection
- Controls for marking, storage, and transport of media
- Media sanitization and downgrading

Legal Advice and Advocacy (LGA)

DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)

The PCI Secure SLC Standard outlines security requirements and assessment procedures for software vendors to validate how they properly manage the security of payment software throughout the entire software lifecycle. This course provides baseline knowledge needed to implement security requirements and assessment procedures to validate proper management of the security of payment software throughout the entire software lifecycle.

After completing this course you will be able to:

- Identify and mitigate common threats and vulnerabilities defined in the PCI Secure SLC standard
- Build an environment for secure software development, change control, and management
- Improve communications for secure deployment, configuration and software updates.

ENG 151 – Fundamentals of Privacy Protection (10 mins)

Staying current on legislation and engaging the business on timely privacy compliance and practical solutions can be challenging. As the focus on compliance continues to increase, and the GRC landscape continues to evolve, compliance officers need to keep pace with emerging regulations. This course provides learners with a clear understanding of their role in meeting compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Enable better privacy engineering practices that support privacy by design concepts
- Ensure collaboration on privacy protection objectives across your organization
- Apply the NIST Privacy Framework to meet region-specific regulations such as GDPR and CCPA
- Communicate privacy practices with individuals, business partners, assessors, and regulators

---

TST 206 – ASVS Requirements for Developers (20 mins)

Ensuring developers understand application security needs can be overwhelming, but leveraging OWASP ASVS organizations can test and prove applications meet specific levels of security. This course is designed to equip Privacy and Cybersecurity Management with the knowledge required to provide development teams with a basis for testing web application technical security controls and a list of requirements for secure development in adherence to the Application Security Verification Standard (ASVS) 3.0 standard.

Upon successful completion of this course, learners will have the knowledge and skills required to meet ASVS compliance requirements, including:

- Using the ASVS to audit applications and to establish both internal and procurement metrics
- Understanding the role of ASVS Levels and Threat profiles
- Providing the necessary guidance and training to ensure your organization meets ASVS requirements.

Network Services (NET)

COD 252 – Securing Google Platform Applications & Data (COMING SOON) (25 mins)

Google Cloud Platform adoption provides many organizations with the agility and scalability needed to transform their business but lack of awareness surrounding best security practices and control implementation increases the risk of a security breach. This course provides the knowledge and skills to implement and leverage GCP security features, manage secrets, and protect applications and data against common threats.

Topics Include:

- Google Cloud Platform security features
- Creating, managing, and protecting secrets
- Common security threats
- Google Cloud monitoring and auditing facilities.

COD 287 – Java Application Server Hardening (20 mins)

This secure operations and maintenance course introduce best practices for server hardening.

Topics Include:

- Minimizing unnecessary privileges and functionality
- Being current with dependencies and server software
- Protecting connections and data in transit

DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)

The adoption of cloud services involves various roles making it difficult to govern the selection and brokering of cloud services while adhering to policies and procedures. This course is designed to ensure privacy and security teams may effectively and efficiently adopt cloud computing in support of strategic and business goals.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Creating Policies, Procedures, Standards, and Controls that meet all regulatory and legal requirements, industry standards, and technical controls such as encryption.
- Establishing, deploy and assess a compliance baseline that determines targets
- Handling sensitive data, including how to identify and classify data, define data retention periods, and comply with data storage requirements.
- Prepare for compliance auditing and Reporting

DES 210 – Hardening Linux/Unix Systems (30 mins)

Hardening is a critical step in ensuring security and diligence as it reduces the chances of attack, but this requires the use of appropriate methodologies. In today's connected world securing an operating system has become increasingly sophisticated as computing ecosystems increase in complexity. This course provides learners with an understanding of best practices for hardening Linux and Unix systems.

After completing this course you will be able to:

- Upgrade your kernel
- Disable root cron jobs

- Enforce strict firewall rules
- Disable unnecessary services
- Check for backdoors and rootkits
- Check listening ports
- Monitor and manage logs using IDS

DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)

This course is designed for Network Operations Specialists and aligns with the NICE requirements for the secure planning, implementation, and operation of network services and systems, including hardware and virtual environments.

Coverage includes:

- Security Principles
- Network Topologies
- Demilitarized Zones
- Routers, Switches, Bridges, and Firewalls
- Wireless Access Points
- Transmission Media
- Network Authentication
- Server Configuration

DES 215 – Defending Infrastructure (UPDATED) (30 mins)

This course is designed for the System Administrator role and aligns with the NICE requirements for system administration on specialized cyber defense applications and systems (e.g, antivirus, audit, and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.

DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)

This course provides DevOps Engineers, IT Architects and Network Engineers responsible for the security of applications and data with the skills and knowledge required to protect their organization's cloud infrastructure.

Topics Include:

- The role of Data Encryption
- Identity and Authentication
- Firewalls and Network Security (SDNs, VPNs, DMZs)
- Division of Duties
- Compliance requirements
- Securing VM and Containers

DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)

Using Microservices, organizations can isolate software functionality into multiple independent modules that are individually responsible for performing precisely defined, standalone tasks communicating with each other through simple, universally accessible application programming interfaces (APIs). Containers enable developers to simultaneously build and ship these microservices; integrate them with other systems and automatically orchestrate them using predefined rules and processes.

This course is designed to educate DevOps Engineers, IT Architects, and Network Engineers working in Linux or on the cloud to add value to the application lifecycle through proper orchestration and enable faster development and fault-prone provisioning and configurations.

Topics Include:

- Hardening the OS
- Vulnerability Scanning
- Docker, SELinux and AWS Microservices
- API Gateways
- Node monitoring with Prometheus
- Implementing OAuth

- Schedulers and Orchestrators
- Defining a Pod Security Policy
- Using Metadata Concealment

DSO 256 – DevSecOps in the Google Cloud Platform (COMING SOON) (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure Google Cloud Services to meet the NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.
Upon successful completion of this course, you will have the knowledge and skills to:

- Use Identity and Access Controls to define, enforce, and manage user access policies with Google Cloud Identity and Access Management (IAM)
- Develop strategies for integrating security into your DevOps pipeline
- Use different strategies for securing pipeline resources
- Understand different methods for protecting secrets used in deployment applications

---

SDT 323 – Improper Input Validation (10 mins)

Input validation is used to check potentially dangerous inputs but when software does not validate this input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-20 by the 2020 CWE Top 25.

Topics include:

- Identifying malicious input
- Recognizing the impact of this vulnerability
- Strategies for defending against Improper Input Validation
- Testing for Improper Input Validation weaknesses

Operate & Maintain (OM)

COD 141 – Fundamentals of Database Security (30 mins)

In practice, the database represents the goal of many attackers, as this is where the information of value is maintained. However, the functional requirements and security testing often focus on the interaction between a software user and the application, while the handling of data is assumed to be secure.

This course describes how to apply authentication and access control to your database and provides an understanding of database privileges and limiting data access. Coverage also includes techniques for protecting the database and methods for securely concealing specific data while providing an introduction to cloud databases and database encryption.

COD 252 – Securing Google Platform Applications & Data (COMING SOON) (25 mins)

Google Cloud Platform adoption provides many organizations with the agility and scalability needed to transform their business but lack of awareness surrounding best security practices and control implementation increases the risk of a security breach. This course provides the knowledge and skills to implement and leverage GCP security features, manage secrets, and protect applications and data against common threats.

Topics Include:

- Google Cloud Platform security features
- Creating, managing, and protecting secrets
- Common security threats
- Google Cloud monitoring and auditing facilities.

COD 287 – Java Application Server Hardening (20 mins)

This secure operations and maintenance course introduce best practices for server hardening.

Topics Include:

- Minimizing unnecessary privileges and functionality
- Being current with dependencies and server software
- Protecting connections and data in transit

DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)

The adoption of cloud services involves various roles making it difficult to govern the selection and brokering of cloud services while adhering to policies and procedures. This course is designed to ensure privacy and security teams may effectively and efficiently adopt cloud computing in support of strategic and business goals.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Creating Policies, Procedures, Standards, and Controls that meet all regulatory and legal requirements, industry standards, and technical controls such as encryption.
- Establishing, deploy and assess a compliance baseline that determines targets
- Handling sensitive data, including how to identify and classify data, define data retention periods, and comply with data storage requirements.
- Prepare for compliance auditing and Reporting

DES 210 – Hardening Linux/Unix Systems (30 mins)

Hardening is a critical step in ensuring security and diligence as it reduces the chances of attack, but this requires the use of appropriate methodologies. In today's connected world securing an operating system has become increasingly sophisticated as computing ecosystems increase in complexity. This course provides learners with an understanding of best practices for hardening Linux and Unix systems.

After completing this course you will be able to:

- Upgrade your kernel
- Disable root cron jobs
- Enforce strict firewall rules
- Disable unnecessary services
- Check for backdoors and rootkits
- Check listening ports
- Monitor and manage logs using IDS

DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)

This course is designed for Network Operations Specialists and aligns with the NICE requirements for the secure planning, implementation, and operation of network services and systems, including hardware and virtual environments.

Coverage includes:

- Security Principles
- Network Topologies
- Demilitarized Zones
- Routers, Switches, Bridges, and Firewalls
- Wireless Access Points
- Transmission Media
- Network Authentication
- Server Configuration

DES 215 – Defending Infrastructure (UPDATED) (30 mins)

This course is designed for the System Administrator role and aligns with the NICE requirements for system administration on specialized cyber defense applications and systems (e.g, antivirus, audit, and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.

DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)

This course provides DevOps Engineers, IT Architects and Network Engineers responsible for the security of applications and data with the skills and knowledge required to protect their organization's cloud infrastructure.

Topics Include:

- The role of Data Encryption
- Identity and Authentication
- Firewalls and Network Security (SDNs, VPNs, DMZs)
- Division of Duties
- Compliance requirements
- Securing VM and Containers

DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)

Using Microservices, organizations can isolate software functionality into multiple independent modules that are individually responsible for performing precisely defined, standalone tasks communicating with each other through simple, universally accessible application programming interfaces (APIs). Containers enable developers to simultaneously build and ship these microservices; integrate them with other systems and automatically orchestrate them using predefined rules and processes.

This course is designed to educate DevOps Engineers, IT Architects, and Network Engineers working in Linux or on the cloud to add value to the application lifecycle through proper orchestration and enable faster development and fault-prone provisioning and configurations.

Topics Include:

- Hardening the OS
- Vulnerability Scanning
- Docker, SELinux and AWS Microservices
- API Gateways
- Node monitoring with Prometheus
- Implementing OAuth
- Schedulers and Orchestrators
- Defining a Pod Security Policy
- Using Metadata Concealment

DSO 256 – DevSecOps in the Google Cloud Platform (COMING SOON) (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure Google Cloud Services to meet the NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.
Upon successful completion of this course, you will have the knowledge and skills to:

- Use Identity and Access Controls to define, enforce, and manage user access policies with Google Cloud Identity and Access Management (IAM)
- Develop strategies for integrating security into your DevOps pipeline
- Use different strategies for securing pipeline resources
- Understand different methods for protecting secrets used in deployment applications

---

DSO 303 – Automating Security Updates (20 mins)

Essential to keeping systems secure, reducing risk, introducing new or enhanced features, or improving compatibility, software updating can be challenging and resource-intensive. Automating this process eliminates routine tasks and frees up administrative time. This course introduces automation procedures for systems administration to effectively and efficiently manage IT software in adherence to functional and security requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Employ automated mechanisms to implement changes to the current system baseline and deploy the updated baseline across the installed base
- Review system changes to determine whether unauthorized changes have occurred
- Remove previous versions of software or firmware components after installing updated versions
- Ensure that security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures

---

DSO 305 – Automating CI/CD Pipeline Compliance (20 mins)

The adoption of cloud infrastructure and DevOps requires consistent integration of security to achieve a reliable lifecycle of continuous deployment. Integrating compliance into the CI/CD Pipeline requires a coordinated effort by everyone involved in the development pipeline. This course enables learners to automate the implementation of security tasks across the CI/CD pipeline in adherence to compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Automate scanning and reporting tasks to ensure privacy policies, applicable laws, regulations, and service-level agreements are reviewed and documented for compliance regulations
- Identify and document controls owned by outside parties
- Configure change monitors to identify changes to organizational systems and environments of operation that may affect security and privacy risk
- Verify that all control objectives are met, and all key controls are designed and operating effectively

---

ENG 110 – Essential Account Management Security (15 mins)

This infrastructure security course provides essential guidance on implementing specific account management security controls at the hardware and software level to facilitate compliance with applicable regulatory requirements.

Topics include:

- How to define and control network access
- Creating a separation of duties policy
- Building and managing segregation of resources strategies
- Monitoring system access
- Using digital certificates for authentication

ENG 111 – Essential Session Management Security (15 mins)

This infrastructure security course provides guidance to system designers and developers on how to implement session management controls at the software level. These techniques enhance security of web applications and facilitates compliance with applicable regulatory requirements.

Topics include:

- Securing session identifiers
- Implementing Transport Layer Security (TLS) so sensitive data is always transmitted over secure channels
- Ensuring client browsers send cookies over HTTPS connections

---

ENG 112 – Essential Access Control for Mobile Devices (15 mins)

This infrastructure security course teaches designers and developers how to implement software-level access controls on mobile devices to mitigate threats, protect privacy, and comply with applicable regulatory requirements.

Topics include:

- Identifying threats to mobile devices
- The importance of protecting user privacy and confidentiality
- Methods for encrypting data at rest and data in transit

- Implementing application code signing to ensure software integrity

---

ENG 113 – Essential Secure Configuration Management (15 mins)

This infrastructure security course trains program managers, system designers, and developers on proper security practices for defining and implementing IT system configuration management.

Topics include:

- Key configuration practices and configuration change control
- Security impact analysis
- Access restrictions for change
- Principle of least functionality
- Information system component inventory

ENG 119 – Essential Security Audit & Accountability (15 mins)

This infrastructure security course trains information system owners, system administrators, and information system security officers on how to build and communicate effective audit policies and controls.

Topics include:

- Documenting security audits
- Implementing audit controls
- Using audit tools
- Generating audit reports

ENG 121 – Essential Identification & Authentication (15 mins)

This infrastructure security course teaches those responsible for information security how to develop identification and authentication policy and controls. The course spans personnel, devices, and information systems.

Topics include:

- Identification and authentication of users inside and outside your organization
- Device identification and authentication
- Identifier management
- Authenticator management and feedback
- Cryptographic module authentication
- Service identification and authentication
- Adaptive identification and authentication
- Processes for re-authentication

ENG 122 – Essential Physical & Environmental Protection (15 mins)

This infrastructure security course educates those responsible for developing physical and environmental protection policies how to create effective controls and comply with applicable regulatory requirements.

Topics include:

- Physical access authorizations and control
- Access control for transmission medium and output devices
- Monitoring physical access
- Information leakage, asset monitoring and tracking

ENG 125 – Essential Data Protection (15 mins)

This infrastructure security course delivers training to personnel in information systems, information security, systems design, software development, and IT operations on essential data security techniques. Focus is primarily on cryptographic controls at the information systems level and compliance with applicable regulatory requirements.

Topics include:

- Asymmetric key algorithms
- Using hash functions to protect data integrity
- Proper password storage for authentication purposes
- Encrypting file transfers and downloads
- Adding salt values before hashing
- Using Certificate Authorities

ENG 127 – Essential Media Protection (15 mins)

This infrastructure security course describes the development and dissemination of an organization-wide information media protection policy that addresses scope, roles, responsibilities, and coordination among organizational entities to facilitate compliance with applicable regulatory requirements.

Topics include:

- Best practices for media protection
- Controls for marking, storage, and transport of media
- Media sanitization and downgrading

SDT 323 – Improper Input Validation (10 mins)

Input validation is used to check potentially dangerous inputs but when software does not validate this input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-20 by the 2020 CWE Top 25.

Topics include:

- Identifying malicious input
- Recognizing the impact of this vulnerability
- Strategies for defending against Improper Input Validation
- Testing for Improper Input Validation weaknesses

Oversee & Govern (OV)

AWA 101 – Fundamentals of Application Security (30 mins)

This course introduces the fundamentals and primary drivers of application security.

Topics include:

- Core concepts of application security risk management
- Anatomy of an application attack
- Common attack scenarios juxtaposed with key security principles
- Best practices for developing secure applications

AWA 102 – Secure Software Concepts (30 mins)

This course provides a high-level overview of secure software concepts for web applications including application security, security standards, secure development methodologies, and security best practices.

Topics include:

- Current application security threat landscape
- Common security vulnerabilities
- Evaluating and mitigating the most common application security risks
- Security-related tasks for each stage in the software development lifecycle
- How to implement a security strategy based on your organization’s risk

---

COD 102 – The Role of Software Security (10 mins)

This course introduces you to the overriding importance of software security for your organization, and the potential business consequences of developing and deploying insecure software.

Topics include:

- The difference between software security and network security
- Business imperatives for software security, including the high business costs of security breaches
- Compliance and legal implications of security breaches
- Customer expectations of security
- The increasing threat landscape

COD 103 – Creating Software Security Requirements (10 mins)

This course discusses the requirements phase of the software development lifecycle and provides software development teams with the knowledge and skill required to gather security requirements for the software that they are designing and implementing.

Topics Include:

- Identifying potential attacks and exploits
- Legal Security Requirements
- Business Requirements
- Customer Security Requirements

COD 104 – Designing Secure Software (15 mins)

This course provides learners with the skill and knowledge required to perform threat modeling, and ensure that security principles are applied at each step of the design process.

Topics Include:

- Integrating attack surface reduction
- Secure defaults
- Least privilege
- Defense in depth
- Compartmentalization

COD 105 – Secure Software Development (20 mins)

This course introduces you to secure development models, standards, and guidelines that provide you with a structure for reducing risk from application security vulnerabilities.

Topics Include:

- The role of Industry standards and security models like OWASP Top 10, CWE SANS Top 25, PA-DSS and many more
- The common criteria for Information Technology Security Education
- Formal methods applied to the analysis of software to ensure that it adheres to industry standards such as Code Analysis, Static Analysis, and Binary Analysis

---

COD 106 – The Importance of Software Integration and Testing (15 mins)

This course introduces you to the Integration and Testing phases of the software development lifecycle, including the roles of Code Review, Fault Injection, Vulnerability Scanning, Penetration Testing, and Static Analysis.

Topics Include:

- Pros and cons of performing a code review
- Resources available when conducting a code review
- Identifying vulnerabilities that may have been missed by other secure testing techniques

- Utilizing fault injection
- Vulnerability Scanning and Penetration Testing
- Pros and cons of static analysis

COD 107 – Secure Software Deployment (10 mins)

This course describes general principles to think about for improving your deployment process, best practices for logging and monitoring, as well as different ways to defend the operating system, web server and the database.

After complicating this course you will understand attack surface reduction, compartmentalization, defense in depth, least privilege deployment, secure defaults and security incident response plans.

COD 108 – Software Operations and Maintenance (10 mins)

This course covers best practices for logging and monitoring, as well as security misconfiguration and mitigation techniques.

After completing this course you will understand application security patching processes, strategies for defense-in-depth, and mechanisms to ensure sufficient logging and monitoring.

DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)

The PCI Secure SLC Standard outlines security requirements and assessment procedures for software vendors to validate how they properly manage the security of payment software throughout the entire software lifecycle. This course provides baseline knowledge needed to implement security requirements and assessment procedures to validate proper management of the security of payment software throughout the entire software lifecycle.

After completing this course you will be able to:

- Identify and mitigate common threats and vulnerabilities defined in the PCI Secure SLC standard
- Build an environment for secure software development, change control, and management
- Improve communications for secure deployment, configuration and software updates.

DES 305 – Protecting Existing Blockchain Assets (20 mins)

Blockchain implementation poses a number of challenges from storage capacity and scalability to anonymity and data privacy thus making the protection of existing assets complex. This course provides learners with an understanding of how to secure existing Blockchain assets against security threats.

After completing this course you will be able to:

- Secure the cryptographic keys that allow access to the ledger
- Use hardware security modules (HSMs)
- Ensure the integrity of “Smart Contracts”
- Protect communications between nodes

DSO 201 – Fundamentals of Secure DevOps (30 mins)

Building a culture of collaboration between software development (Dev) and information-technology operations (Ops) is full of challenges and learning. The notion of DevOps requires a good understanding of complex technical problems and business needs at the same time. This course introduces learners to the philosophy and provides the fundamental knowledge needed to execute practices that shorten system development lifecycles and provide continuous delivery with high software quality.

After completing this course you will be able to:

- Understand the unique opportunities for including security in your DevOps pipeline
- Understand at which points in your development process—from architecture to deployment—you can improve security
- Automate security compliance and controls using a variety of open-source tools
- Identify opportunities for increased collaboration and better feedback loops

---

DSO 205 – Securing the COTS Supply Chain (15 mins)

The usage of Commercial-off-the-shelf software (COTS) by organizations while advantageous comes with its own set of challenges and complexities. Unfortunately, it is rare for acquisition approaches to account for complex software supply chains; this course provides learners with an understanding of how to apply DevSecOps best practices to reduce software supply chain risks.

After completing this course you will be to:

- Employ acquisition strategies, contract tools, and procurement methods for the purchase of the software, COTS from suppliers
- Conduct a supplier review prior to entering into a contractual agreement to acquire the COTS
- Conduct an assessment of the COTS prior to selection, acceptance, or update
- Employ security safeguards to validate that the COTS received is genuine and has not been altered
- Establish and retains the unique identification of supply chain elements, processes, and actors for the COTS
- Establish a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements

---

DSO 206 – Securing the Open Source Supply Chain (15 mins)

As modern software development evolves, organizations are finding themselves leveraging Open Source Software to reduce costs, simplify operations, accelerate innovation, and improve interoperability. Adoption is expected to continue, but distribution and licenses allow anyone to use, view, modify, and share source code, which introduces new security vulnerability risks into the supply chain. This course provides learners with an understanding of how to apply DevSecOps best practices to reduce software supply chain risks inherent with the use of open-source software.

After completing this course you will be to meet compliance requirements while developing a DevSecOps mindset, including:

- Expanding the development teams use of dependency checking tools, including integration into the build process
- Ensuring application security teams implement security tests to audit select open-source software and components
- Establishing a build process that ensures the installation of the latest open software releases for operations teams migrating server platforms to containers
- Understanding the importance of monitoring repo feeds and CVEs, especially critical libraries such as OpenSSL that could affect many different products

---

ENG 151 – Fundamentals of Privacy Protection (10 mins)

Staying current on legislation and engaging the business on timely privacy compliance and practical solutions can be challenging. As the focus on compliance continues to increase, and the GRC landscape continues to evolve, compliance officers need to keep pace with emerging regulations. This course provides learners with a clear understanding of their role in meeting compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Enable better privacy engineering practices that support privacy by design concepts
- Ensure collaboration on privacy protection objectives across your organization
- Apply the NIST Privacy Framework to meet region-specific regulations such as GDPR and CCPA
- Communicate privacy practices with individuals, business partners, assessors, and regulators

---

TST 206 – ASVS Requirements for Developers (20 mins)

Ensuring developers understand application security needs can be overwhelming, but leveraging OWASP ASVS organizations can test and prove applications meet specific levels of security. This course is designed to equip Privacy and Cybersecurity Management with the knowledge required to provide development teams with a basis for testing web application technical security controls and a list of requirements for secure development in adherence to the Application Security Verification Standard (ASVS) 3.0 standard.

Upon successful completion of this course, learners will have the knowledge and skills required to meet ASVS compliance requirements, including:

- Using the ASVS to audit applications and to establish both internal and procurement metrics
- Understanding the role of ASVS Levels and Threat profiles
- Providing the necessary guidance and training to ensure your organization meets ASVS requirements.

Project Management/Acquisition and Program (PMA)

AWA 101 – Fundamentals of Application Security (30 mins)

This course introduces the fundamentals and primary drivers of application security.

Topics include:

- Core concepts of application security risk management
- Anatomy of an application attack
- Common attack scenarios juxtaposed with key security principles
- Best practices for developing secure applications

AWA 102 – Secure Software Concepts (30 mins)

This course provides a high-level overview of secure software concepts for web applications including application security, security standards, secure development methodologies, and security best practices.

Topics include:

- Current application security threat landscape
- Common security vulnerabilities
- Evaluating and mitigating the most common application security risks
- Security-related tasks for each stage in the software development lifecycle
- How to implement a security strategy based on your organization's risk

---

COD 102 – The Role of Software Security (10 mins)

This course introduces you to the overriding importance of software security for your organization, and the potential business consequences of developing and deploying insecure software.

Topics include:

- The difference between software security and network security
- Business imperatives for software security, including the high business costs of security breaches
- Compliance and legal implications of security breaches
- Customer expectations of security
- The increasing threat landscape

COD 103 – Creating Software Security Requirements (10 mins)

This course discusses the requirements phase of the software development lifecycle and provides software development teams with the knowledge and skill required to gather security requirements for the software that they are designing and implementing.

Topics Include:

- Identifying potential attacks and exploits
- Legal Security Requirements
- Business Requirements
- Customer Security Requirements

COD 104 – Designing Secure Software (15 mins)

This course provides learners with the skill and knowledge required to perform threat modeling, and ensure that security principles are applied at each step of the design process.

Topics Include:

- Integrating attack surface reduction
- Secure defaults
- Least privilege

- Defense in depth
- Compartmentalization

COD 105 – Secure Software Development (20 mins)

This course introduces you to secure development models, standards, and guidelines that provide you with a structure for reducing risk from application security vulnerabilities.

Topics Include:

- The role of Industry standards and security models like OWASP Top 10, CWE SANS Top 25, PA-DSS and many more
- The common criteria for Information Technology Security Education
- Formal methods applied to the analysis of software to ensure that it adheres to industry standards such as Code Analysis, Static Analysis, and Binary Analysis

---

COD 106 – The Importance of Software Integration and Testing (15 mins)

This course introduces you to the Integration and Testing phases of the software development lifecycle, including the roles of Code Review, Fault Injection, Vulnerability Scanning, Penetration Testing, and Static Analysis.

Topics Include:

- Pros and cons of performing a code review
- Resources available when conducting a code review
- Identifying vulnerabilities that may have been missed by other secure testing techniques
- Utilizing fault injection
- Vulnerability Scanning and Penetration Testing
- Pros and cons of static analysis

COD 107 – Secure Software Deployment (10 mins)

This course describes general principles to think about for improving your deployment process, best practices for logging and monitoring, as well as different ways to defend the operating system, web server and the database.

After complicating this course you will understand attack surface reduction, compartmentalization, defense in depth, least privilege deployment, secure defaults and security incident response plans.

COD 108 – Software Operations and Maintenance (10 mins)

This course covers best practices for logging and monitoring, as well as security misconfiguration and mitigation techniques.

After completing this course you will understand application security patching processes, strategies for defense-in-depth, and mechanisms to ensure sufficient logging and monitoring.

DES 151 – Fundamentals of the PCI Secure SLC Standard (25 mins)

The PCI Secure SLC Standard outlines security requirements and assessment procedures for software vendors to validate how they properly manage the security of payment software throughout the entire software lifecycle. This course provides baseline knowledge needed to implement security requirements and assessment procedures to validate proper management of the security of payment software throughout the entire software lifecycle.

After completing this course you will be able to:

- Identify and mitigate common threats and vulnerabilities defined in the PCI Secure SLC standard
- Build an environment for secure software development, change control, and management
- Improve communications for secure deployment, configuration and software updates.

DES 305 – Protecting Existing Blockchain Assets (20 mins)

Blockchain implementation poses a number of challenges from storage capacity and scalability to anonymity and data privacy thus making the protection of existing assets complex. This course provides learners with an understanding of how to secure existing Blockchain assets against security threats.

After completing this course you will be able to:

- Secure the cryptographic keys that allow access to the ledger
- Use hardware security modules (HSMs)
- Ensure the integrity of “Smart Contracts”
- Protect communications between nodes

DSO 201 – Fundamentals of Secure DevOps (30 mins)

Building a culture of collaboration between software development (Dev) and information-technology operations (Ops) is full of challenges and learning. The notion of DevOps requires a good understanding of complex technical problems and business needs at the same time. This course introduces learners to the philosophy and provides the fundamental knowledge needed to execute practices that shorten system development lifecycles and provide continuous delivery with high software quality.

After completing this course you will be able to:

- Understand the unique opportunities for including security in your DevOps pipeline
- Understand at which points in your development process—from architecture to deployment—you can improve security
- Automate security compliance and controls using a variety of open-source tools
- Identify opportunities for increased collaboration and better feedback loops

---

DSO 205 – Securing the COTS Supply Chain (15 mins)

The usage of Commercial-off-the-shelf software (COTS) by organizations while advantageous comes with its own set of challenges and complexities. Unfortunately, it is rare for acquisition approaches to account for complex software supply chains; this course provides learners with an understanding of how to apply DevSecOps best practices to reduce software supply chain risks.

After completing this course you will be to:

- Employ acquisition strategies, contract tools, and procurement methods for the purchase of the software, COTS from suppliers
- Conduct a supplier review prior to entering into a contractual agreement to acquire the COTS
- Conduct an assessment of the COTS prior to selection, acceptance, or update
- Employ security safeguards to validate that the COTS received is genuine and has not been altered
- Establish and retains the unique identification of supply chain elements, processes, and actors for the COTS
- Establish a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements

---

DSO 206 – Securing the Open Source Supply Chain (15 mins)

As modern software development evolves, organizations are finding themselves leveraging Open Source Software to reduce costs, simplify operations, accelerate innovation, and improve interoperability. Adoption is expected to continue, but distribution and licenses allow anyone to use, view, modify, and share source code, which introduces new security vulnerability risks into the supply chain. This course provides learners with an understanding of how to apply DevSecOps best practices to reduce software supply chain risks inherent with the use of open-source software.

After completing this course you will be to meet compliance requirements while developing a DevSecOps mindset, including:

- Expanding the development teams use of dependency checking tools, including integration into the build process
- Ensuring application security teams implement security tests to audit select open-source software and components
- Establishing a build process that ensures the installation of the latest open software releases for operations teams migrating server platforms to containers
- Understanding the importance of monitoring repo feeds and CVEs, especially critical libraries such as OpenSSL that could affect many different products

---

ENG 151 – Fundamentals of Privacy Protection (10 mins)

Staying current on legislation and engaging the business on timely privacy compliance and practical solutions can be challenging. As the focus on compliance continues to increase, and the GRC landscape continues to evolve, compliance officers need to keep pace with emerging regulations. This course provides learners with a clear understanding of their role in meeting compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Enable better privacy engineering practices that support privacy by design concepts
- Ensure collaboration on privacy protection objectives across your organization
- Apply the NIST Privacy Framework to meet region-specific regulations such as GDPR and CCPA
- Communicate privacy practices with individuals, business partners, assessors, and regulators

---

TST 206 – ASVS Requirements for Developers (20 mins)

Ensuring developers understand application security needs can be overwhelming, but leveraging OWASP ASVS organizations can test and prove applications meet specific levels of security. This course is designed to equip Privacy and Cybersecurity Management with the knowledge required to provide development teams with a basis for testing web application technical security controls and a list of requirements for secure development in adherence to the Application Security Verification Standard (ASVS) 3.0 standard.

Upon successful completion of this course, learners will have the knowledge and skills required to meet ASVS compliance requirements, including:

- Using the ASVS to audit applications and to establish both internal and procurement metrics
- Understanding the role of ASVS Levels and Threat profiles
- Providing the necessary guidance and training to ensure your organization meets ASVS requirements.

Protect & Defend (PR)

ATK 201 – Using the MITRE ATT&CK Framework (15 mins)

The MiTRE ATT& CK Framework is a knowledge base of globally observed adversary tactics and techniques. This course provides an understanding of behaviors that may be used for developing threat models, mapping threats, classifying attacks, or training both red and blue teams.

Topics Include:

- The purpose of the ATT&CK Framework
  Structures, tactics, and techniques within the framework
- Using the ATT&CK Framework to detect and analyze threats
- Mitigation best-practices for preventing attacks

DSO 301 – Orchestrating Secure System and Service Configuration (20 mins)

Building and maintaining quality software requires functional configuration management, but this is easier said than done in today's day and age. This process involves automation, but minimizing errors while securely and systematically managing changes in systems is complicated. This course provides Systems Developers, Network Operations Specialists, System Administrators, and Systems Security Analysts with the necessary skills to consistently and securely manage environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Identifying and mitigating gaps in your current orchestration security policies
- Ensuring the coordination and consistency of security policies across the enterprise
- The importance of maintaining immutability of live container instances, ensuring that changes occur in the source control and are only deployed via new versions of the resource
- Understanding the role of third-party tools such as Clair, Actuary, and Anchore in testing Infrastructure-as-Code (IAC) and Configuration-as-Code (CAC) platforms

---

ENG 118 – Essential Incident Response (15 mins)

This infrastructure security course teaches incident response policy development and the associated controls to help ensure appropriate communication and action throughout your organization.

Topics include:

- Incident response testing
- Incident handling
- Incident monitoring
- Incident reporting

ENG 211 – How to Create Application Security Design Requirements (15 mins)

To preserve the confidentiality, integrity, and availability of application data, software applications must be engineered with security in mind. Without defined security requirements, design choices will be made without security guidance and security testing cannot be effective.

This course provides technical and non-technical personnel with the knowledge to understand, create, and articulate security requirements as part of a software requirement document.

Topics include:

- Applying the application security maturity (ASM) model to the development process
- Key security engineering activities: gathering security objectives, applying security design guidelines, and creating threat models
- Identifying threats, attacks, vulnerabilities, and countermeasures
- How to conduct impactful security architecture and design reviews to identify potential security problems and minimize the application's attack surface.

ENG 311 – Attack Surface Analysis & Reduction (25 mins)

The attack surface of an application represents the number of entry points exposed to a potential attacker. The larger the attack surface, the larger the set of methods that can be used by an adversary breaking into software applications. Resultantly, minimizing it is a key exercise in risk reduction.

Topics covered:

- Understanding the goals and methodologies of attackers
- Identifying attack vectors that expose the application
- Defining and reducing an application's attack surface

TST 202 – Penetration Testing Fundamentals (25 mins)

Serving as a comprehensive way of testing for cybersecurity vulnerabilities Penetration Testing provides insight into a network, application, device, and/or physical security through the lens of an attacker to discover weaknesses and identify areas of improvement within your security posture. This course introduces concepts of penetration testing and provides an understanding of the stages of penetration testing as they relate to industry standards.

After completing this course, you will be able to:

- Conduct penetration testing according to an industry-standard methodology
- Identify the steps in a typical penetration testing process

---

TST 301 – Infrastructure Penetration Testing (45 mins)

Reliance on IT systems, regulatory compliance, and the evolving cyberthreat landscape are key indicators of the importance of Infrastructure penetration testing. Infrastructure Penetration tests can help inform cybersecurity strategies, validate existing security controls, and identify weaknesses in need of improvement. This course provides learners with the skills and knowledge necessary to perform penetration tests that simulate how attackers might attempt to compromise the organization's infrastructure.

After completing this course you will be able to:

- Perform pretest identification of potential vulnerabilities based on pretest analysis
- Leverage automated scanning tools

- Establish a baseline indication of the potential attack surface of the environment
- Interpret the results of automated tools to determine what additional testing is needed
- Perform host discovery, port scanning, and network segmentation checks
- Analyze the results of the penetration test are then compiled into a report

---

TST 302 – Application Penetration Testing (45 mins)

Applications store, process, and transmit data making them susceptible and vulnerable to hackers who can identify and exploit vulnerabilities. Penetration testing of these applications acts as a safeguard to reduce vulnerabilities and attack surface. This course provides learners with the skills and knowledge necessary to perform penetration tests that simulate how attackers might attempt to compromise the software applications.

After completing this course you will be able to:

- Conduct planning and reconnaissance
- Scan to understand how the target application will respond to various intrusion attempts
- Gain access using web application attacks, such as cross-site scripting, SQL injection, and backdoors, to uncover a target's vulnerabilities
- Maintain access to determine if the vulnerability can be used to achieve a persistent presence in the exploited system
- Analyze the results of the penetration test are then compiled into a report

---

TST 351 – Penetration Testing for TLS Vulnerabilities (12 mins)

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. However, flaws in TLS protocol include weak cryptographic primitives, or specific implementation errors, cross-protocol vulnerabilities, or any combination of each. This course teaches how to identify vulnerabilities, detecting acceptance of unencrypted connections, and testing configurations.

After completing this course, you will be able to:

- Identify typical TLS misconfiguration vulnerabilities
- Detect network services accepting unencrypted connections
- Test web server TLS configuration

TST 352 – Penetration Testing for Injection Vulnerabilities (12 mins)

Stemming from improperly sanitized or completely unsensitized input injection flaws allow attackers to relay malicious code through an application to another system. This course teaches how to identify and test for these vulnerabilities within your code.

After completing this course, you will be able to:

- Identify common injection vulnerabilities
- Test for command injection vulnerabilities
- Detect code and XML injection vulnerabilities
- Exploit command and code injection vulnerabilities

TST 353 – Penetration Testing for SQL Injection (12 mins)

Used to attack data-driven applications in which malicious SQL statements are inserted into an entry field for execution SQL Injection allows attackers to conduct a number of malicious activities to data including but not limited to becoming administrators of the database server. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Test for the presence of SQL Injection vulnerabilities
- Exploit SQL Injection vulnerabilities
- Identify the common tools and techniques used to exploit SQL Injection vulnerabilities

---

TST 354 – Penetration Testing for Memory Corruption Vulnerabilities (12 mins)

Occurring when the contents of a memory location are modified due to programmatic behavior that exceeds the intention of the original programmer or program/language constructs. This type of programming error can lead to a program crash or strange and bizarre program behavior. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Identify common memory corruption vulnerabilities
- Test for buffer overflows + Exploit known memory corruption vulnerabilities
- Understand advanced techniques for finding memory corruption vulnerabilities

---

TST 355 – Penetration Testing for Authorization Vulnerabilities (12 mins)

Authorization is the process of enforcing policies; determining what types of qualities of activities, resources, or services a user is permitted. Authorization vulnerabilities include forceful browsing and privilege escalation. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Identify common authorization vulnerabilities
- Test application access controls
- Exploit authorization vulnerabilities

TST 356 – Penetration Testing for Cross-Site Scripting (XSS) (12 mins)

Cross-site Scripting (XSS) is a client-side code injection attack where the attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Define the types of Cross-Site Scripting vulnerabilities
- Test applications for Cross-Site Scripting vulnerabilities
- Exploit Cross-Site Scripting vulnerabilities

TST 357 – Penetration Testing for Hardcoded Secrets (12 mins)

All modern applications rely on certain secrets to run from database connection strings to API keys or cryptographic keys. Keeping these secrets is critical to the security of the application as they typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This course teaches how to identify and test for the use of hard-coded credentials.

After completing this course, you will be able to:

- Determine whether an application contains hard-coded authentication credentials
- Determine whether an application contains hard-coded cryptographic keys
- Find plain-text secrets in application binaries
- Find leaked secrets in code repositories
- Identify techniques for advanced testing of application code for the presence of hard-coded secrets

---

TST 358 – Penetration Testing Wireless Networks (12 mins)

Wireless networks have security issues that are vulnerable to various attacks. Organizations need to proactively search out any weakness in security if they are to avoid unauthorized access to network resources and data leakage. This course introduces tools and techniques while teaching how to Identify and test for common attacks.

After completing this course, you will be able to:

- Test for the presence of unauthorized wireless networks
- Identify common attacks on wireless networks
- Identify the common tools and techniques for testing wireless networks

---

TST 359 – Penetration Testing Network Infrastructure (12 mins)

Essential to every organization; Infrastructure penetration testing provides an opportunity to know about the current situation of a company and analyze existing potential breach points. The process includes all internal computer systems, associated external devices, internet networking, cloud, and virtualization testing. This course teaches how to perform Network Infrastructure penetration tests, perform necessary scans, and test controls.

After completing this course, you will be able to:

- Perform network-layer penetration tests
- Test network segmentation controls
- Perform a network scan to discover active devices
- Perform a port scan on a host to identify exposed network services

---

TST 360 – Penetration Testing for Authentication Vulnerabilities (12 mins)

Building authentication and session management schemes correctly is a difficult task often presenting flaws that may equally difficult to Identify. Common authentication attacks consist of brute force, insufficient authentication, and weak password recovery validation. These types of attacks target and attempt to exploit the authentication process a web site uses to verify the identity of a user, service, or application. This course teaches how to execute attacks, identify vulnerabilities, and verify controls.

After completing this course, you will be able to:

- Identify common authentication vulnerabilities
- Verify authentication controls
- Execute dictionary attacks

Risk Management (RSK)

COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software, system components, and custom software. The software should be tested regularly to ensure security controls continue to reflect a changing environment.

In this course, you will learn how to ensure critical data can only be accessed by authorized personnel and develop an understanding of systems and processes that must be in place to limit access based on a need to know and according to job responsibilities. Additionally, you will learn how to test security controls and ensure they continue to reflect a changing environment.

DES 212 – Architecture Risk Analysis & Remediation (30 mins)

This course defines concepts, methods, and techniques for analyzing the architecture and design of a software system for security flaws. Special attention is given to analysis of security issues in existing applications; however, the principles and techniques are applicable to systems under development. Techniques include accurately capturing application architecture, threat modeling with attack trees, attack pattern analysis, and enumeration of trust boundaries.

Topics include:

- How to assess design components for security flaws
- The use and value of threat modeling and attack surface analysis
- Techniques to remove architecture weak spots and avoid vulnerability propagation

---

DES 222 – Applying OWASP 2017: Mitigating Injection (12 mins)

In this course, you will learn how to mitigate the risks associated with injection, as defined by OWASP.

After completing this course, you will understand how to:

- Keep data separate from commands and queries
- Implement multi-factor authentication
- Require weak-password checks

- Limit login attempts

DES 223 – Applying OWASP 2017: Mitigating Broken Authentication (12 mins)

In this course, you will learn how to mitigate the risks associated with broken authentication, as defined by OWASP.
After completing this course, you will understand how to:

- Use secure coding best practices to confirm user identity
- Implement strong authentication mechanisms
- Protect user sessions and session data

DES 224 – Applying OWASP 2017: Mitigating Sensitive Data Exposure (12 mins)

In this course, you will learn how to mitigate the risks associated with sensitive data exposure, as defined by OWASP.

After completing this course, you will understand how to:

- Enforce the use of up-to-date and strong standards-based crypto algorithms
- Properly store passwords using strong adaptive and salted hashing functions
- Encrypt data in transit with secure protocols

DES 225 – Applying OWASP 2017: Mitigating XML External Entities (12 mins)

In this course, you will learn how to mitigate the risks associated with XML External Entities (XXE), as defined by OWASP.

After completing this course, you will understand how to:

- Apply secure coding practices to avoid serialization of sensitive data
- Patch all XML processors and libraries
- Implement server-side input validation

DES 226 – Applying OWASP 2017: Mitigating Broken Access Control (12 mins)

In this course, you will learn how to mitigate the risks associated with broken access control, as defined by OWASP.

After completing this course, you will understand how to:

- Implement access control policies
- Assess the effectiveness of current access controls
- Employ secure coding practices to ensure users cannot act outside intended permissions

---

DES 227 – Applying OWASP 2017: Mitigating Security Misconfiguration (12 mins)

In this course, you will learn how to mitigate the risks associated with security misconfiguration, as defined by OWASP.

After completing this course, you will understand how to:

- Segment application architecture
- Implement a concerted, repeatable application security configuration process
- Code defensively to avoid misconfiguration problems in deployment

---

DES 228 – Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (12 mins)

In this course, you will learn how to mitigate the risks associated with Cross-Site Scripting (XSS), as defined by OWASP.

After completing this course, you will understand how to:

- Leverage secure frameworks
- Implement secure coding practices to avoid XSS attacks
- Escape untrusted HTTP requests

- Apply context-sensitive encoding to separate untrusted data from active browser content

---

DES 229 – Applying OWASP 2017: Mitigating Insecure Deserialization (12 mins)

In this course, you will learn how to mitigate the risks associated with insecure deserialization, as defined by OWASP.

After completing this course, you will understand how to:

- Implement integrity checks such as digital signatures
- Apply secure coding practices for serialized objects
- Enforce strict type constraints
- Effectively restrict network connectivity

DES 230 – Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (12 mins)

In this course, you will learn how to mitigate the risks associated with using components with known vulnerabilities, as defined by OWASP.

After completing this course, you will understand how to:

- Monitor applications for out of date components
- Triage and apply updates for known vulnerabilities
- Apply secure coding practices over the lifetime of an application

---

DES 231 – Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (12 mins)

In this course, you will learn how to mitigate the risks associated with insufficient logging and monitoring, as defined by OWASP.

After completing this course, you will understand how to:

- Ensure all login, access failures, and input validation failures are logged
- Implement sufficient user context to identify suspicious behavior
- Allow sufficient time so malicious accounts can be tracked for forensic analysis
- Apply best practices for secure application logging

DES 271 – OWASP M1: Mitigating Improper Platform Usage (12 mins)

In this course, you will learn how to mitigate the risks associated with Improper Platform Usage which might include Android intents, platform permissions, misuse of TouchID, the keychain, or some other security control that is part of the mobile operating system.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to improper platform usage
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 272 – OWASP M2: Mitigating Insecure Data Storage (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Data Storage which includes threat agents such as an adversary that has attained a lost/stolen mobile device; malware or another repackaged app acting on the adversary's behalf that executes on the mobile device.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insecure data storage
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 273 – OWASP M3: Mitigating Insecure Communication (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Communication which might include threat agents such as an adversary that shares local network (compromised or monitored Wi-Fi); carrier or network devices (routers, cell towers, proxy's, etc); or malware on your mobile device.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insecure communication
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 274 – OWASP M4: Mitigating Insecure Authentication (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Authentication which is typically exploited through automated attacks that use available or custom-built tools.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to Insecure Authentication
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 275 – OWASP M5: Mitigating Insufficient Cryptography (12 mins)

In this course, you will learn how to mitigate the risks associated with Insufficient Cryptography which includes threat agents such as anyone with physical access to data that has been encrypted improperly, or mobile malware acting on an adversary's behalf.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insufficient cryptography
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 276 – OWASP M6: Mitigating Insecure Authorization (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Authorization which allows an adversary to execute functionality they should not be entitled to using an authenticated but lower-privilege user of the mobile app.

After completing this course, you will be able to:

- Identify best practices for implementing secure authorization for Mobile Internet of Things
- How to mitigate the threat of Insecure Authorization
- Identify and mitigate Insecure Direct Object Reference (IDOR) vulnerabilities

---

DES 277 – OWASP M7: Mitigating Client Code Quality (12 mins)

In this course, you will learn how to mitigate the risks associated with poor code quality, including threat agents such as entities that can pass untrusted inputs to method calls made within mobile code.

After completing this course, you will be able to:

- Identify Uncontrolled Format String and Classic Buffer Overflow
- Recognize their potential impact
- Apply coding best practices to avoid them
- Find these weaknesses in your mobile application's source code
- Test your application to detect them

DES 278 – OWASP M8: Mitigating Code Tampering (12 mins)

In this course, you will learn how to mitigate the risks associated with code tampering. Typically, an attacker will exploit code modification via malicious forms of the apps hosted in third-party app stores. The attacker may also trick the user into installing the app via phishing attacks.

After completing this course, you will be able to:

- Identify code tampering vulnerabilities
- Defend against code tampering attacks

DES 279 – OWASP M9: Mitigating Reverse Engineering (12 mins)

In this course, you will learn how to mitigate risks associated with reverse engineering in which an attacker will typically download the targeted app from an app store and analyze it within their local environment using a suite of different tools.

After completing this course, you will be able to:

- Describe what kinds of knowledge reverse engineering may reveal to an attacker
- List mitigation techniques for reverse engineering

DES 280 – OWASP M10: Mitigating Extraneous Functionality (12 mins)

In this course, you will learn how to mitigate the risks associated with extraneous functionality. Typically, an attacker seeks to understand extraneous functionality within a mobile app in order to discover hidden functionality in backend systems. The attacker will typically exploit extraneous functionality directly from their own systems without any involvement by end-users.

After completing this course, you will be able to:

- Identify Extraneous Functionality
- Understand how an attacker might exploit this vulnerability in your software
- Mitigate exposure to this threat

DES 281 – OWASP IoT1: Mitigating Weak, Guessable or Hardcoded Passwords (12 mins)

In this course, you will learn how to mitigate the risks associated with the use of easily brute-forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

When you have completed this course, you will be able to:

- Identify best practices for implementing secure authentication for the Internet of Things
- Identify and mitigate password weaknesses in your applications

---

DES 282 – OWASP IoT2: Mitigating Insecure Network Services (12 mins)

In this course, you will learn how to mitigate the risks associated with unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.

After you have completed this course, you will be able to:

- Identify best practices to protect network services on IoT devices, including:
    - Only open necessary ports
    - Do not overexpose ports
    - Block unusual traffic
    - Mitigate DoS vulnerabilities
    - Mitigate memory corruption vulnerabilities|Disable outdated protocols

---

DES 283 – OWASP IoT3: Mitigating Insecure Ecosystem Interfaces (12 mins)

In this course, you will learn how to mitigate the risks associated with insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

After completing this course, you will be able to:

- Identify common threats to IoT web interfaces

- Apply best practices to mitigate these threats

DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

After you have completed this course, you will be able to:

- List the steps of a typical update process
- Describe how to protect update connections
- Explain how to protect the update server
- List the steps to securely sign and verify an update
- Evaluate whether Secure Boot is necessary for your device at this time
- Identify types of sensitive data that should not be included in updates
- Securely implement transport encryption for an Internet of Things (IoT) system

---

DES 285 – OWASP IoT5: Mitigating Use of Insecure or Outdated Components (12 mins)

In this course, you will learn how to mitigate the risks associated with the use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms and the use of third-party software or hardware components from a compromised supply chain.

After you have completed this course, you will be able to identify and mitigate threats posed by insecure and outdated components.

DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection (12 mins)

In this course, you will learn how to mitigate the risks associated with a user's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

After completing this course, you will learn to:

- Identify threats to personal information
- Identify ways to protect personal information

DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

After completing this course, you will be able to:

- Identify missing encryption
- Recognize the potential impact of this security defect
- Apply best practices to prevent insecure data transfer and storage

---

DES 288 – OWASP IoT8: Mitigating Lack of Device Management (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanism.

After completing this course, you will be able to:

- Monitor and Track Assets
- Monitor, Handle and Retain Information
- Monitor and Control System and Network Access

DES 289 – OWASP IoT9: Mitigating Insecure Default Settings (12 mins)

In this course, you will learn how to mitigate the risks associated with devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

After you have completed this course, you will be able to understand insecure default settings and their mitigation techniques.

DES 290 – OWASP IoT10 Mitigating Lack of Physical Hardening (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

After completing this course, you will be able to:

- Understand fail-safe defaults
- Use best practices for hardening

DES 312 – Protecting Cardholder Data (20 mins)

While cardholder data consists of any personally identifiable information (PII) associated with a person who has a credit or debit card, the PCI Secure Standards Council (PCI SSC) has specific requirements to protect cardholder data at all times. Despite common misconceptions, this also includes account numbers, expiration date, and/or service code as cardholder data. This course is designed to provide Information Systems Security Developers with the knowledge needed to minimize the storage of cardholder data and take necessary precautions to protect it in adherence to the PCI Software Security Framework and NIST 800-53 Guidelines.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Ensuring the software does not store sensitive authentication data after authorization, even if encrypted unless the software is intended only for use by issuers or organizations that support issuing services.
- Rendering the Primary Account Number (PAN) is unreadable anywhere it is stored.
- Guiding customers regarding the secure deletion of cardholder data after the expiration of the customer-defined retention period.

DSO 307 – Secure Secrets Management (20 mins)

As the need to protect critical data increases, organizations must focus efforts on improving processes used to manage essential information. This course is designed to ensure software development teams employ appropriate techniques to manage identities, privileges, and secrets securely.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Ensuring that approved cryptographic algorithms and methods are used for securing critical assets
- Aligning key-management processes and procedures with those recognized by industry-standards bodies
- Using Approved Random Number Generators| Providing strong entropy when Using Random Number Generator

---

ENG 114 – Essential Risk Assessment (15 mins)

This infrastructure security course provides essential guidance on information system risk assessment techniques. Individuals responsible for information systems, IT security, risk management, or oversight responsibilities will find this course valuable. It teaches how to define and manage the purpose, scope, roles, and coordination among organizational entities to help ensure appropriate risk assessment and compliance with applicable regulatory requirements.

Topics include:

- Security categorization
- Risk assessment
- Vulnerability scanning
- The system development lifecycle
- Security engineering principles
- Developer security testing and evaluation

- Development process, standards, and tools
- Developer security architecture and design
- Component authenticity

ENG 150 – Meeting Confidentiality, Integrity, and Availability (30 mins)

The CIA Triad – Confidentiality, Integrity, and Availability are the information security tenets used as a means for analyzing and improving the security of your application and its data. After completing this course, you will be able to understand and use confidentiality, integrity, and availability (CIA) as the three main tenets of information security.

ENG 251 – Risk Management Foundations (20 mins)

Risk management should be a foundational tool used to facilitate thoughtful and purposeful defense strategies. In today's environment, the most significant threats to systems come from purposeful attacks that are often disciplined, well organized, and well-funded.

This course aims to educate IT architects, Analysts, and DevOps Engineers to understand their responsibilities when protecting organizational assets.

Topics Include:

- Key Risk Management Concepts
- Common management techniques and strategies
- various risk assessment methods and risk control strategies

---

ENG 351 – Preparing the Risk Management Framework (20 mins)

Before any organization can adequately Implement the Risk Management Framework they must understand how to determine and apply appropriate security requirements. Preparation requires a disciplined and structured set of activities in order to execute the framework at appropriate risk management levels.

This course aims to provide Engineers, Software Architects, and Systems Analysts with context and priorities for managing security and privacy risk.

Topics Include:

- Identifying key Individuals and specification of roles and responsibilities in the risk management process
- Identifying risk tolerance and determining a particular strategy for risk management
- Conducting an organization-level risk assessment to ensure leadership is aligned
- Continuous monitoring to enable a rapid and effective response to changes in the risk landscape or changes in the effectiveness of controls

---

ENG 352 – Categorizing Systems and Information within the RMF (10 mins)

Security categorization provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system. This course provides learners with an understanding of how to categorize the system and the information using the NIST SP 800-37 Rev. 2 Risk Management Framework.

After completing this course you will be able to:

- Identify all information types based on the system boundary
- Categorize information (processed, stored, or transmitted) by the potential adverse impact that information being compromised as regards confidentiality, integrity or availability
- Ensure the security categorizations are consistent with roles, operating environment, connectivity, and intended use

---

ENG 353 – Selecting, Implementing and Assessing Controls within the RMF (20 mins)

Selecting the appropriate set of security controls helps to achieve organizational operations and objectives. This course provides learners with an understanding of how to select, implement and assess security controls using the NIST SP 800-37 Rev. 2 Risk Management Framework.

After completing this course you will be able to:

- Select and document the controls necessary to protect the information system and organization commensurate with the risk to the organization
- Implement the controls in the security and privacy plans for the system and organization
- Document the specific details of the control implementation in a baseline configuration
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements

---

ENG 354 – Authorizing and Monitoring System Controls within the RMF (20 mins)

Authorizing and monitoring security controls provides an understanding of security posture and provides an indication of whether or not cybersecurity controls are operating as intended. This course provides learners with an understanding of the Authorization and Monitoring steps of the NIST SP 800-37 Rev. 2 Risk Management Framework.

After completing this course you will be able to:

- Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk to operations, assets, and individuals is acceptable
- Report authorization decisions, significant vulnerabilities, and risks to organizational officials | Monitoring the system and the associated controls on an ongoing basis
- Document changes to the system and environment of operation
- Conduct risk assessments and impact analyses | Reporting the security and privacy posture of the system

---

TST 205 – Performing Vulnerability Scans (45 mins)

Performing vulnerability scans is a necessary first step to evaluating the security of an organization's network and helping protect organizational data and assets; this includes assessing, mitigating, and reporting on any security vulnerabilities that exist in an organization's systems and software.

Topic includes:

- Enumerating Platforms, Software Flaws, and improper configurations
- Formatting Checklists and test procedures
- Measuring vulnerability impact
- Analyzing vulnerability scan reports and results from security control assessments

---

Securely Provision (SP)

COD 110 – Fundamentals of Secure Mobile Development (45 mins)

This course introduces developers to mobile environment threats and risks and presents secure programming principles to mitigate them.

Topics include:

- Common threats to mobile applications: client-side injection, sensitive data handling, network transition, application patching, web-based attacks, phishing, third-party code, location security and privacy and denial of service
- Defensive coding techniques: input validation, output encoding, least privilege, code signing, data protection at rest and in transit, avoiding client side validation, and using platform security capabilities as they apply in mobile environments
- Threat modeling of mobile applications

COD 152 – Fundamentals of Secure Cloud Development (20 mins)

This course introduces developers to the common risks associated with Cloud applications and secure coding best practices to mitigate them.

Topics include:

- Security features of the different series models (IaaS, PaaS, and SaaS)
- How to identify common vulnerabilities and code defensively to avoid them

- Common threats to cloud applications: unauthorized account access, insecure APIs, shared technology, data leakage, and account hijacking
- Complying with regulatory requirements
- The unique security challenges of “Big Data”
- How to apply the Microsoft SDL (https://siwpestage.wpengine.com/course-category/standard/ms-sdl/) to cloud applications

---

COD 160 -Fundamentals of Secure Embedded Software Development (45 mins)

Embedded devices tend to be linked to other devices via a wide array of technologies and often susceptible to targeted attacks. This course identifies security issues inherent to embedded devices and their deployment environments. You will also learn about the appropriate constraint of functionality from a security standpoint, and techniques to prevent common vulnerabilities.

Topics include:

- Techniques to identify system security and performance requirements
- Developing appropriate security architecture
- Selecting the correct mitigations
- How to develop policies that can ensure the secure operation of your system

---

COD 170 – Identifying Threats to Mainframe COBOL Applications & Data (20 mins)

This secure coding course covers the most common security issues that affect the confidentiality, integrity and availability of COBOL programs on mainframes. These include SQL Injection, Command Injection, Integer Overflow, Weak Cryptography, Unencrypted Communications and Race Conditions.

COD 201 – Secure C Encrypted Network Communications (15 mins)

This course explores secure communications using Transport Layer Security (TLS) and best practices for implementing these within C and C++ applications.

Topics include:

- Key principles of TLS
- Libraries and interfaces for implementing the TLS protocol
- TLS security considerations
- Alternatives to TLS

COD 202 – Secure C Runtime Protection (15 mins)

This secure coding course covers common run-time protection technologies that can be used to protect an application from attack.

Topics include:

- Run-time protection technologies and how to apply them to your applications
- Stack security cookies, Address Space Layout Randomization (ASLR), and No-eXecute (NX)
- Limitations of run-time protection technologies

COD 206 – Creating Secure C++ Code (15 mins)

This secure coding course highlights the most useful security features for avoiding memory corruption vulnerabilities in C++.

Additional topics include:

- Standard containers, bounds-checking functions, smart pointers, and standard concurrency features
- How to use object-oriented programming features to define and manipulate data in terms of objects, use range-based loops and native regular expressions

---

COD 207 – Communication Security in C++ (15 mins)

This secure coding course focuses on how to protect data in transit using encryption libraries and strong TLS ciphers in C++.

Topics include:

- Important issues about public key certificates including signing and verification
- Using well-trusted encryption libraries and strong TLS cipher suites to protect data in transit
- Protect and verify the integrity of public key certificates

---

COD 214 – Creating Secure GO Applications (30 mins)

As organizations continue to migrate to cloud infrastructures; development teams are finding themselves leveraging GO as a tool of choice. Lightweight and quick to compile due to generous libraries and abstractions that make it easier to program concurrent and distributed (read: cloud) applications it offers a slew of benefits from Static compilation with no dependencies, a strong standard library, a full development environment, and the ability to build for multiple architectures with no minimal hassle.

This course will provide software developers and DevOps Engineers with working knowledge of fundamental concepts and advanced features of the GO programming language.

Topics Include:

- Identifying and preventing SQL injection attacks
- Understanding cross-site scripting
- Properly configuring browser cookies
- Understanding and preventing session hijacking attacks
- Knowing how to avoid cross-site request forgery vulnerabilities
- Understanding the difference between symmetric and asymmetric cryptography
- Implementing transport layer security
- Working with hashes and key derivation functions

*Indicates that the course is still in production and subject to change

---

COD 216 – Leveraging .NET Framework Code Access Security (CAS) (30 mins)

This course explores the foundation of .NET, the CLR's native security infrastructure (Code Access Security), and the ASP.NET security infrastructure.

Topics include:

- Differences between managed and unmanaged code
- Access control functions in Windows
- Code Access Security (CAS) functions in .NET
- Interactions between Windows access control and CAS
- Key aspects of ASP.NET security and understand the Level 2 Security Transparency Model

---

COD 217 – Mitigating .NET Security Threats (45 mins)

With a primary focus on .NET secure error handling and secure logging, this course describes secure coding techniques to avoid information disclosure and other vulnerabilities.

Topics include:

- Avoiding dangerous patterns when using CAS
- Avoiding common .NET security pitfalls
- Ensuring application fail safely

COD 219 – Creating Secure Code: SAP ABAP Foundations (90 mins)

This secure coding course presents best practices and techniques for secure SAP application development using Java and ABAP.

Topics include:

- Key application security principles, vulnerabilities and mitigations

- Validating input in SAP applications
- Protecting data using encryption
- Conducting security code analysis and code reviews

COD 241 – Creating Secure Oracle DB Applications (45 mins)

This secure coding course introduces database application developers to key industry best practices for data security.

Topics include:

- Secure query construction
- Secure communication and storage
- Creating safe stored procedures to prevent SQL Injection
- How to secure data at rest and data in transit using Oracle Database features

---

COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)

This secure coding course explores protecting sensitive data and ensuring the integrity of applications running on the Microsoft SQL Server Engine and Azure SQL Database.

Topics include:

- The security function of roles in controlling user and principal access to SQL Server securables
- Exercising fine-grained controls that adhere to the Principle of Least Privilege
- Leveraging the security features of Microsoft's Azure SQL Database to protect sensitive data and ensure the integrity of your applications

---

COD 246 – PCI DSS 3: Protecting Stored Cardholder Data (15 mins)

In this course, you will learn how to use the CWE-311 guidelines to identify, test and mitigate for missing encryption of sensitive data. Coverage includes techniques for spotting missing encryption through code review and testing. Secure coding best practices are included, as well as descriptions of technology-specific weaknesses as appropriate. This course requires basic knowledge of client-server applications, web applications, the Software Development Life Cycle, cryptography, and the STRIDE model.

COD 247 – PCI DSS 4: Encrypting Transmission of Cardholder Data (15 mins)

In this course, you will learn about the risks of insecure communications and how to use the CWE guidelines, specifically the OWASP Top Ten, to mitigate these risks. Coverage includes techniques for spotting missing encryption and using Transport Layer Security (TLS).

COD 248 – PCI DSS 6: Develop and Maintain Secure Systems and Applications (15 mins)

In this course, you will learn to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities. Coverage will be aligned with the CWE SANS Top 25 and OWASP 2017 Top 10 vulnerability frameworks.

COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software, system components, and custom software. The software should be tested regularly to ensure security controls continue to reflect a changing environment.

In this course, you will learn how to ensure critical data can only be accessed by authorized personnel and develop an understanding of systems and processes that must be in place to limit access based on a need to know and according to job responsibilities. Additionally, you will learn how to test security controls and ensure they continue to reflect a changing environment.

COD 251 – Defending AJAX-Enabled Web Applications (25 mins)

This course introduces fundamentals of how to defend AJAX-enabled Web applications, including the difference between regular and AJAX-enabled web applications, AJAX security checks against challenges, and common attacks against AJAX-enabled applications.

Topics include:

- Architectural differences between regular web applications and AJAX-enabled applications
- Identifying threats to AJAX applications: cross-site scripting (XSS), cross-site request forgery (CSRF), and injection attacks
- Implementing countermeasures against attacks: protecting client resources, validating input, protecting web services requests, preventing request forgeries, and securing data access.

COD 253 – Creating Secure AWS Cloud Applications (45 mins)

This course examines the security vulnerabilities, threats, and mitigations for AWS cloud computing services and provides best practices for securing Web applications by leveraging AWS platform security features.

Topics include:

- AWS security features: Key Management Service (KMS), Hardware Security Module (HSM), Identity and Access Management (IAM), and CloudWatch
- How to leverage security features built into Common Amazon Cloud services such as Simple Storage Service (S3), Elastic Compute Cloud (Amazon EC2), Elastic Block Store (EBS), Amazon Glacier, Relational Database Service (RDS), DynamoDB, Elastic MapReduce (EMR), and Amazon Machine Images (AMI)

COD 254 – Creating Secure Azure Applications (45 mins)

This course examines key Azure security platforms and services that you can use to improve the security of your applications.

Topics include:

- Security vulnerabilities, threats, and mitigations for Azure cloud computing services
- How to identify common security threats to cloud-based applications
- Secure coding best practices to mitigate threats
- How to leverage built-in Azure features for an extra layer of defense

---

COD 255 – Creating Secure Code: Web API Foundations (20 mins)

This secure coding course introduces the fundamentals of secure web services development.

Topics include:

- Common web services threats that put your application at risk
- Impact of web services attacks
- Secure development best practices to protect web services

COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Ruby on Rails. After completing this course, you will be able to identify and mitigate injection vulnerabilities, such as SQL injection and cross-site scripting, build strong session management into your Rails applications, and prevent other common vulnerabilities, such as cross-site request forgery and direct object access.

Topics include:

- How to identify and mitigate injection vulnerabilities: SQL Injection (SQLi) and cross-site scripting (XSS)
- How to build strong session management into your rails applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF) and direct object access

---

COD 257 – Creating Secure Python Web Applications (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Python. After completing this course, you will be able to understand various types of injection vulnerabilities, including SQL injection and cross-site scripting. You will also be able to understand how to build strong session management into your Python web applications and how to prevent common vulnerabilities, such as cross-site request forgery, direct object access, and others.

Finally, you will be able to recognize file system threats to web applications, including vulnerabilities with path traversal, temporary files, and insecure client redirects.

Topics include:

- Types of Injection Vulnerabilities including SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- File system threats to web applications including vulnerabilities with path traversal, temporary files, and insecure client redirects
- How to build strong session management into your python web applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF), direct object access, and others

---

COD 258 – Creating Secure PHP Web Applications (30 mins)

In this course, you will learn important concepts for secure PHP scripting. After completing this course, you will be able to use quotation marks correctly, discuss techniques for handling return codes and exceptions, canonicalize paths to identify the correct files, identify dangerous functions to avoid, apply techniques for preventing or mitigating different injection vulnerabilities, recognize that regular expressions must be handled carefully to avoid DoS attacks, and describe techniques to protect sensitive data in transit.

Topics covered:

- Key defensive coding principles such as proper session management, error handling, authentication, authorization, data storage, and use of encryption
- Avoiding and mitigating vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), File Inclusion, Command Injection, Cross-Site Request Forgery (CSRF) and Null Byte attacks

---

COD 259 – Node.js Threats & Vulnerabilities (30 mins)

In this secure coding course, you will learn about system configuration, injection attacks, session management, package management, and the AngularJS framework, all within the context of Node.js security.

Topics include:

- Best practices for Node.js server and system configuration
- Types of injection attacks and mitigation techniques
- Proper settings for session cookie security
- Mitigating cross-site request forgery (CSRF) attacks
- Leveraging popular static analysis tools for Node.js
- Understand why templates and expressions are vulnerable to injection
- Methods, services, elements, and parameters that should not be used with untrusted data
- Best practices for loading templates

COD 261 – Threats to Scripts (30 mins)

In this secure coding course, you will learn about the impact of incorrect script development or lax security measures.

Topics include:

- Outcomes of vulnerable scripts
- Common scripting vulnerabilities such as SQL Injection (SQLi)
- Security issues related to permissions and privileges
- Impact of different types of resource

COD 262 – Fundamentals of Shell and Interpreted Language Security (30 mins)

In this secure coding course, you will learn about how shell scripting languages compare with more modern interpreted languages with respect to security features, and defensive coding techniques, and dealing with common differences between platforms that can alter script behavior.

Topics incude:

- Information security principles including least privilege and defense in depth
- The importance of data validation and how to validate using input, array indices, and environment variables
- Using file system operations safely to protect
- Preventing or mitigating cached secret disclosure
- The importance of up-to-date communication security techniques
- Operating system (OS) system portability issues

COD 263 – Secure Bash Scripting (15 mins)

In this secure coding course, you will learn about the importance of error and exception handling in shell scripts and interpreted languages such as Perl, Python, Bash and Ruby.

Topics covered:

- Techniques for handling errors and exceptions in shell scripts and interpreted languages
- Common syntax pitfalls and dangerous functions to avoid
- Techniques for preventing/mitigating different vulnerabilities including different types of injection

---

COD 264 – Secure Perl Scripting (15 mins)

Perceived as being difficult to fix in comparison to other programming languages Perl is commonly known as “the duct-tape of the Internet.” This general-purpose programming language is currently being used for a wide range of tasks as it takes the best features from other languages.

In this course, you will learn about best practices for secure scripting in Perl, features of Perl’s taint mode, handling errors in Perl, protecting files, preventing format string and injection vulnerabilities, using regular expressions carefully, and protecting sensitive data in transit with Transport Layer Security (TLS).

COD 265 – Secure Python Scripting (15 mins)

In this secure coding course, you will learn important concepts for secure Python scripting including techniques for error and exception handling.

Topics Covered:

- Avoiding uncontrolled format string vulnerabilities
- Defending against Regular Expression Denial of Service (DoS) attacks
- Protecting sensitive data in transit
- Techniques for preventing/mitigating different vulnerabilities including different types of injection

---

COD 266 – Secure Ruby Scripting (15 mins)

In this secure coding course, you will learn important concepts for secure Ruby scripting, techniques for preventing/mitigating different vulnerabilities including different types of injection, and protecting sensitive data in transit.

Topics covered:

- Validating command-line parameters
- Using quotation marks correctly
- Using unmask to set default file permissions
- Protecting files and canonicalizing paths
- Defending against Regular Expression Denial of Service (DoS) attacks

---

COD 267 – Securing Python Microservices (30 mins)

Microservices have become widely popular, replacing complicated XML-based schemas and service-oriented architectures (SOA) because of the ability to create separate, well-defined, individual components within a system. By leveraging python microservices, complex applications can be broken down into these components to ease further development and deployment.

This course will provide cloud developers, python developers, and software architects with a working knowledge of possible attacks, how to secure interaction between services and an understanding of how to implement basic principles to ensure the security of python microservices.

Topics Include:

- Techniques for handling return codes and exceptions
- Canonicalizing paths to identify the correct files
- Identifying dangerous functions
- Applying techniques for mitigating injection vulnerabilities
- How to securely handle regular expressions
- How to protect sensitive data

COD 270 – Creating Secure COBOL & Mainframe Applications (25 mins)

This secure coding course covers countermeasures for security vulnerabilities on mainframe systems such as input validation, parameterized APIs, strong cryptography, and memory management issues.

Topics include:

- Identifying vulnerabilities and threats to mainframe applications and data
- Mitigating SQL injection threats using safe prepared statements and parameterized APIs
- Validating all input
- Using exec* functions instead of system functions to mitigate the risk of command injection
- Using key derivation functions to protect stored password
- Encrypting sensitive data at rest using AES-256
- Protecting sensitive data in transit with TLS
- Preventing deadlocks by using the ENQ and DEQ commands
- Avoiding manual memory management in order to prevent buffer overflow conditions

---

COD 281 – Java Security Model (20 mins)

In this secure coding course, you will learn about Java's policy-driven security model and how to leverage it to build more secure applications.

Topics include:

- Java security model components
- Functions of the Java security manager and access controller
- Java security policies and the Java security policy files

COD 283 – Java Cryptography (45 mins)

This secure coding course explores the key concepts of public key cryptography and teaches you how to use the Java keytool command-line utility for creating and managing keys and keystores.

Topics include:

- How public and private key pairs work together to encrypt and decrypt data for secure transfer and to create and verify digital signature
- Generating secure encryption keys and identifying related issues such as pseudo random number generators (PRNGs), key derivation functions, and initialization vectors
- Selecting an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode

---

COD 284 – Secure Java Coding (30 mins)

In this course, you will learn about secure Java coding practices, including techniques for avoiding Denial of Service (DoS) and regular expression DoS attacks, and guidelines for secure error handling and logging. You will also become familiar with the dangers of unreleased resources, null references, and XML external entity (XXE) attacks

Topics include:

- Denial of Service and designing your application to handle or avoid such situations
- Guidelines for secure error handling and logging
- Identify the dangers of unreleased resources, null references, and XML external entity attacks

---

COD 285 – Developing Secure Angular Applications (30 mins)

Widely adopted amongst the software development community because of the versatility it provides, securing angular applications comes with a steep learning curve. While component-based architecture is one of the key benefits of using angular, managing components can be complicated. This course is designed to develop the skills required to design, build, and maintain secure Angular applications following software assurance best practices.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure Angular.js compliance requirements, including:

- Securing AngularJS templates to help mitigate threats from expression Injection and dynamically loading templates from untrusted sources
- Ensuring that both the server and the client cooperate to eliminate these threats and potential security issues that need to be blocked
- Implementing Content Security Policies and secure routing

COD 286 – Creating Secure React User Interfaces (10 mins)

This JavaScript library has become a popular choice in the market because of its ability to help solve web development challenges. The framework makes it painless to create interactive user interfaces, design simple view, and reactively update to changes. This course is designed to develop the skills required to securely build user interfaces using multiple components and implement best practices to avoid common attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure React.js User Interfaces compliance requirements, including:

- Creating secure React components
- Avoiding vulnerable third-party React component libraries
- Preventing React component injection attacks
- Using and serializing JSON

COD 301 – Secure C Buffer Overflow Mitigations (45 mins)

This course focuses on C-language buffers. Upon completion of this course you will learn good memory management techniques and coding best practices to help you avoid buffer & integer overflows, format string vulnerabilities, and race conditions.

Topics include:

- Mitigating buffer overflows and race conditions
- Preventing memory management, format string, injection and integer overflow vulnerabilities
- Protecting data in memory

COD 302 -Secure C Memory Management (20 mins)

This secure coding course focuses on memory manipulation and allocation techniques for C-language software development.

Topics include:

- Key concepts of dynamic memory management
  Common mistakes that lead to Out of Range Memory Access
- Best practices to mitigate memory management vulnerabilities
- How to ensure that “freed” or “deleted” data in memory is no longer accessible

---

COD 303 – Common C Vulnerabilities & Attacks (20 mins)

In this secure coding course, you will review common C application vulnerabilities, how they manifest in code; as well as techniques and libraries that you can use to mitigate the risk of attack.

After completing this course, you will be able to mitigate risk from the following vulnerabilities:

- Format string attacks
- Integer overflows
- Path Traversal issues
- Command injection
- SQL injection

COD 307 – Protecting Data in C++ (25 mins)

This secure coding course presents key concepts of public key cryptography, the risks of improper encryption, and defensive coding techniques to protect sensitive data.

Topics include:

- Generating strong encryption keys and identifying related issues such as pseudo random number generators (PRNGs), key derivation algorithms, and initialization vectors
- Selecting an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode
- Common libraries that support symmetric cryptography
- How public and private key pairs work together both to encrypt and decrypt data for secure transfer and to create and verify digital signatures
- Best practices to mitigate memory exposure vulnerabilities

COD 308 – Common ASP.NET MVC Vulnerabilities and Attacks (45 mins)

This course provides an overview of code security issues that affect ASP.NET MVC applications. You will also understand how other vulnerabilities can be mitigated with careful and complete input validation.

After completing this course, you will be able to understand model validation and its strengths and weaknesses, understand and prevent unique attacks, such as under-posting and over-posting, and implement protective measures against SQL injection, cross-site scripting, cross-site request forgery, and malicious URL redirects.

COD 309 – Securing ASP.NET MVC Applications (30 mins)

This course teaches the fundamentals of authentication and authorization in ASP.NET Web API, and the roles they play in the OWIN pipeline.

After completing this course, you will understand:

- Web API pipeline and where each component sits on that path
- Authentication and authorization filters and the role of each in your Web API application
- Different authentication options and how to implement them in your application
- The importance of secure communication and the use of Transport Layer Security (TLS) to create secure data exchange tunnels.

COD 315 – Preventing Vulnerabilities in iOS Code in Swift (20 mins)

In this secure coding course, you will learn how to code defensively to prevent iOS security vulnerabilities.

Topics Include:

- Mitigation approaches and Implementing Secure Coding Best Practices
- How to leverage iOS and Swift security services to mitigate threats
- Pros and Cons of Biometrics such as Touch ID and Face ID

COD 316 – Creating Secure iOS Code in Objective C (30 mins)

This secure coding course describes techniques for creating secure iOS applications.

Topics include:

- Common vulnerabilities such as exposure of authentication credentials, sensitive data, and other secrets; custom URL scheme abuse; and XML eXternal Entity (XXE) Injection
- Techniques for mitigating vulnerabilities including protecting data at rest with the Data Protection and Common Crypto APIs, mitigating sensitive data exposure in background snapshots, preventing custom URL scheme abuse, and mitigating XXE Injection

---

COD 317 – Protecting Data on iOS in Swift (20 mins)

In this secure coding course, you will learn how to code defensively to protect data on iOS

Topics Include:

- Protecting data in transit and at Rest
- App Transport Security (ATS and default settings
- Use of Valid Certificates and Certificate Pinning
- Using URL Loading System to establish Network Connections
- iOS Cryptography Framework and Data Protection Features

COD 318 – Protecting Data on Android in Java (20 mins)

In this secure coding course, you will learn how to protect data on Android applications using Java.

Topics include:

- Protecting Data in transit using Transport Layer Security (TLS)
- Protecting Data at rest using Symmetric Key Encryption
- Using Android KeyStor to Protect Data
- Dangers of External Storage on Android

COD 319 – Preventing Vulnerabilities in Android Code in Java (20 mins)

In this secure coding course, you will learn to meet Android security quality standards using Java.

Topics include:

- Restricting access to Interprocess Communications and shared data
- Applying the Principle of Least Privilege and deferring permissions
- Avoiding disclosure of sensitive data
- Reducing attack vectors for Cross-Site Scripting (XSS)
- Keeping all libraries and dependencies current

COD 321 – Protecting C# from Integer Overflows & Canonicalization (30 mins)

This secure coding course describes methods that will produce secure C# applications.

Topics include:

- Common security vulnerabilities such as Canonicalization Issues and Integer Overflows
- Unique features of C# and the .NET Framework that can be used to mitigate them
- Understand where and when canonicalization issues and integer overflows are likely to occur
- Avoiding common pitfalls

COD 322 – Protecting C# from SQL Injection (8 mins)

This secure coding course presents SQL Injection vulnerabilities and the features of the .NET Framework that can be used to mitigate them.

Topics include:

- Where and when SQL injection is likely to occur
- Avoiding common pitfalls when defending against SQL injection
- Defense-in-Depth Strategies and best practices for mitigating injection vulnerabilities

---

COD 323 – Using Encryption with C# (20 mins)

This secure coding course describes techniques to protect data both in transit and at rest in C# applications using strong cryptography.

Topics include:

- How to protect data using the Data Protection API (DPAPI)
- Avoiding common cryptographic pitfalls
- Protecting sensitive data in transit
- Alternatives to Transport Layer Security (TLS)

COD 324 – Protecting C# from XML Injection (8 mins)

This secure coding course presents XML Injection vulnerabilities and the features of the .NET Framework that can be used to mitigate them.

Topics include:

- Where and when XML injection is likely to occur
- Avoiding common pitfalls when defending against XML injection
- Defense-in-Depth Strategies and best practices for mitigating injection vulnerabilities

---

COD 352 – Creating Secure JavaScript and jQuery Code (45 mins)

In this secure coding course, you will learn about common client-side vulnerabilities and threats to jQuery applications, and techniques for mitigating them.

Additional topics include:

- How to implement new HTML5 security features to secure jQuery applications
- Best practices to secure local storage and implement Transport Layer Security

---

COD 361 – HTML5 Secure Threats (15 mins)

In this secure coding course, you will learn about security risks introduced by HTML5.

Additional topics include:

- Threats to HTML5 such as cross-site scripting (XSS), cross-site request forgery (CSRF), clickjacking, and threats to user privacy
- Secure coding techniques to mitigating HTML5 threats

COD 362 – HTML5 Built in Security Features (20 mins)

This secure coding course describes important HTML5 security features and how to leverage them to produce more robust applications.

Topics include:

- Implementing Same-Origin Policy, Content Security Policy, Cross-Origin Resource Sharing, and IFrame Sandboxing
- Understanding the limitations of Same-Origin Policy
- Employing best practices to avoid common attacks on HTML5 applications

---

COD 363- Securing HTML5 Data (20 mins)

In this course, you will learn about new features that raise security issues in HTML5 forms, security issues surrounding local data storage, best practices for HTML5 connectivity with the WebSocket API and Server-ent Events, and best practices for the Web Workers, History, Geolocation, and Drag and Drop APIs.

COD 364 – Securing HTML5 Connectivity (20 mins)

In this course, you will learn about best practices for securing connections used by applications that leverage HTML5.

COD 366 – Creating Secure Kotlin Applications (20 mins)

As a prime option for building android applications because of its interoperability with java code, maintainability, reliability, and ability to boost team efficiency, Kotlin is being widely adopted but comes with its own set of challenges as does any technology. This course is designed to ensure learners avoid common mistakes and pitfalls as they leverage vital features and build secure mobile applications using this general-purpose programming language.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Enforcing secure communication by safeguarding the data that you exchange between your app and other apps, or between your app and a website, thereby improving your app's stability and protecting the data that you send and receive.
- Using intents to defer permissions
- Storing all private user data within the device's internal storage (which is sandboxed per app)
- Ensuring the device deletes all files when the user uninstalls an app

---

COD 370- Testing for OWASP 2017: Injection (15 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A1:2017 family of injection security vulnerabilities, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for various injection flaws and mitigation measures to protect against them.

COD 371 – Testing for OWASP 2017: Broken Authentication (12 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A2:2017 security vulnerability broken authentication, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for broken authentication flaws and mitigation measures to protect against them.

COD 372 – Testing for OWASP 2017: Sensitive Data Exposure (12 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A3:2017 security vulnerability sensitive data exposure, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for sensitive data exposure flaws and mitigation measures to protect against them.

COD 373 – Testing for OWASP 2017: XML External Entities (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A4:2017 security vulnerability XML external entities, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for XML external entities flaws and mitigation measures to protect against them.

COD 374 – Testing for OWASP 2017: Broken Access Control (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A5:2017 security vulnerability Broken Access Control, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for broken access control flaws and mitigation measures to protect against them.

COD 375 – Testing for OWASP 2017: Security Misconfiguration (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A6:2017 vulnerability security misconfiguration, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for security misconfiguration flaws and mitigation measures to protect against them.

COD 376 – Testing for OWASP 2017: Cross Site Scripting (XSS) (15 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A7:2017 Cross-Site Scripting (XSS) misconfiguration, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for XSS flaws and mitigation measures to protect against them.

COD 377 – Testing for OWASP 2017: Insecure Deserialization (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A8:2017 Insecure Deserialization vulnerability, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for insecure deserialization flaws and mitigation measures to protect against them.

COD 378 – Testing for OWASP 2017: Use of Components with Known Vulnerabilities (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A9:2017 security vulnerability Using Components with Known Vulnerabilities, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for flaws related to known insecure components and mitigation measures to protect against them.

COD 379 – Testing for OWASP 2017: Insufficient Logging & Monitoring (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A10:2017 Insufficient Logging and Monitoring vulnerability, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for insufficient logging and monitoring flaws and mitigation measures to protect against them.

COD 380 – Preventing SQL Injection in Java (8 mins)

This secure coding course describes ways to remediate and prevent SQL Injection (SQLi) vulnerabilities in your Java application.

Topics Include:

- Identifying data types that require encryption
- Best practices for encryption methods
- Avoiding common encryption errors

COD 381 – Preventing Path Traversal Attacks in Java (8 mins)

This secure coding course describes ways to mitigate security risks from Path Traversal Attacks in your Java application.

Topics Include:

- Identifying Path Traversal Attacks and understanding how they work
- Normalizing, canonicalizing, and validating file paths
- Implementing countermeasures to prevent Path Traversal Attacks

---

COD 382 – Protecting Data in Java (30 mins)

This course discusses protecting data at rest and in transit in Java applications. Several code examples are provided to illustrate key concepts.

After completing this course, you will be able to protect data at rest appropriate cryptographic techniques and protect data in transit with appropriate cryptographic techniques.

COD 383 – Protecting Java Backend Services (30 mins)

Backends are designed for applications that need faster performance, large amounts of addressable memory, and continuous or long-running background processes. The versatility of Java enables developers to design and deliver the right business solutions however their efficiency requires distinctive experiencer and great expertise.

This course aims to provide software developers and DevOps Engineers with the next level understanding of best practices for developing back end frameworks using Java while developing skills necessary to handle user input and build secure systems.

Topics Include:

- The Function of OAuth2 and JWT
- How to leverage the JAAS API
- The advantages of the Spring Security framework
- Validating Length Before Applying RegEx
- Protecting Sensitive Data in Transit Using TLS
- How to identify and protect against SQLi, HQLi, XXE, CSRF, and RegEx DoS attacks

---

COD 384 – Protecting Java from Information Disclosure (8 mins)

This secure coding course describes ways to identify and prevent Information disclosure in your Java application.

Topics Include:

- Identifying common Java information disclosure issues
- Protecting Java applications through improved error messaging
- Best practices for preventing information disclosure
- Audit error handling for information disclosure vulnerability

---

COD 385 – Preventing Race Conditions in Java Code (8 mins)

This secure coding course describes ways to identify and prevent race conditions in your Java application.

Topics Include:

- Common Java race condition issues
- Security risks introduced by race conditions
- Secure protection of temp files
- Best practices for preventing race condition issues

COD 386 – Preventing Integer Overflows in Java Code (8 mins)

This secure coding course describes ways to write code to identify and mitigate risks from integer overflows.

Topics Include:

- Common Integer Overflow security risks and prevention methods
- Precondition Testing, Upcasting, and BigInteger Objects
- Google Guava

- Common Integer Overflow Pitfalls

CYB 301 – Fundamentals of Ethical Hacking (15 mins)

As hackers continue to evolve their techniques organizations must train their employees to test their defenses through various penetration techniques. This course introduces common activities performed during the process of Ethical Hacking and provides a basic foundation of common attack techniques and examples of hacking tools.

Topics Include:

- Understanding authorization and scope that define ethical hacking
- Implementing the penetration testing process
- Fundamentals of attacker techniques and the ATT& CK framework
- An overview of hacking skills and tools knowledge domain

DES 101 – Fundamentals of Secure Architecture (20 mins)

In the past, software applications were created with little thought to the importance of security. Recently, businesses have become more rigorous about how they buy and deploy software as security is a large part of the total cost that risk software applications inherently carry. In this course, you examine the state of the industry from a security perspective, setting the foundation for secure software development.

Topics include:

- Application security architecture principles
- Lessons learned: security disasters in software design
- How to use confidentiality, integrity, and availability to drive better security design decisions

---

DES 202 – Cryptographic Suite Services: Encoding, Encrypting & Hashing (45 mins)

This course presents an overview of the fundamental services provided by cryptographic suites, namely encoding, encrypting, and hashing.

Topics include:

- Encoding and decoding
- Encryption and decryption
- The difference between encoding and encryption
- The value and application of hashing
- Where, when, and how to use crypto

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s): K0018: Knowledge of encryption algorithms.

DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)

This course introduces three important elements of cryptographic systems: random number generation, algorithms and keys.

Topics include:

- The critical role of randomness in cryptography
- Common algorithms to perform cryptographic manipulation of information
- Types and roles of cryptographic keys
- The key management problem
- Common types of digital certificates and its creation process
- Components and roles of a public key infrastructure
- Weaknesses in the digital certificate trust mode
- Mechanisms to manage and distribute cryptographic keys

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 204 – Role of Cryptography in Application Development (15 mins)

This course introduces cryptography and how cryptography can help secure software applications and data. It also provides an overview of common uses of cryptography.

Topics include:

- Identifying relevant cryptographic technologies
- Knowing common “data-in-motion” crypto options and the strengths/weaknesses of each
- Applying common “data-at-rest” crypto options and the strengths/weaknesses of each

---

DES 205 – Message Integrity Cryptographic Functions (45 mins)

This course explains how encrypting and signing a message works, how message authentication codes work, and why a digital signature is superior to a cryptographic hash for validating software integrity.

Topics include:

- Message integrity function is its value
- The difference between a message authentication code and a digital signature
- How a digital signature works
- Encrypting and signing messages
- Message authentication codes
- Digital signature vs. a cryptographic hash for validating software integrity

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 212 – Architecture Risk Analysis & Remediation (30 mins)

This course defines concepts, methods, and techniques for analyzing the architecture and design of a software system for security flaws. Special attention is given to analysis of security issues in existing applications; however, the principles and techniques are applicable to systems under development. Techniques include accurately capturing application architecture, threat modeling with attack trees, attack pattern analysis, and enumeration of trust boundaries.

Topics include:

- How to assess design components for security flaws
- The use and value of threat modeling and attack surface analysis
- Techniques to remove architecture weak spots and avoid vulnerability propagation

---

DES 222 – Applying OWASP 2017: Mitigating Injection (12 mins)

In this course, you will learn how to mitigate the risks associated with injection, as defined by OWASP.

After completing this course, you will understand how to:

- Keep data separate from commands and queries
- Implement multi-factor authentication
- Require weak-password checks
- Limit login attempts

DES 223 – Applying OWASP 2017: Mitigating Broken Authentication (12 mins)

In this course, you will learn how to mitigate the risks associated with broken authentication, as defined by OWASP.
After completing this course, you will understand how to:

- Use secure coding best practices to confirm user identity
- Implement strong authentication mechanisms
- Protect user sessions and session data

DES 224 – Applying OWASP 2017: Mitigating Sensitive Data Exposure (12 mins)

In this course, you will learn how to mitigate the risks associated with sensitive data exposure, as defined by OWASP.

After completing this course, you will understand how to:

- Enforce the use of up-to-date and strong standards-based crypto algorithms
- Properly store passwords using strong adaptive and salted hashing functions
- Encrypt data in transit with secure protocols

DES 225 – Applying OWASP 2017: Mitigating XML External Entities (12 mins)

In this course, you will learn how to mitigate the risks associated with XML External Entities (XXE), as defined by OWASP.

After completing this course, you will understand how to:

- Apply secure coding practices to avoid serialization of sensitive data
- Patch all XML processors and libraries
- Implement server-side input validation

DES 226 – Applying OWASP 2017: Mitigating Broken Access Control (12 mins)

In this course, you will learn how to mitigate the risks associated with broken access control, as defined by OWASP.

After completing this course, you will understand how to:

- Implement access control policies
- Assess the effectiveness of current access controls
- Employ secure coding practices to ensure users cannot act outside intended permissions

---

DES 227 – Applying OWASP 2017: Mitigating Security Misconfiguration (12 mins)

In this course, you will learn how to mitigate the risks associated with security misconfiguration, as defined by OWASP.

After completing this course, you will understand how to:

- Segment application architecture
- Implement a concerted, repeatable application security configuration process
- Code defensively to avoid misconfiguration problems in deployment

---

DES 228 – Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (12 mins)

In this course, you will learn how to mitigate the risks associated with Cross-Site Scripting (XSS), as defined by OWASP.

After completing this course, you will understand how to:

- Leverage secure frameworks
- Implement secure coding practices to avoid XSS attacks
- Escape untrusted HTTP requests
- Apply context-sensitive encoding to separate untrusted data from active browser content

---

DES 229 – Applying OWASP 2017: Mitigating Insecure Deserialization (12 mins)

In this course, you will learn how to mitigate the risks associated with insecure deserialization, as defined by OWASP.

After completing this course, you will understand how to:

- Implement integrity checks such as digital signatures
- Apply secure coding practices for serialized objects
- Enforce strict type constraints
- Effectively restrict network connectivity

DES 230 – Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (12 mins)

In this course, you will learn how to mitigate the risks associated with using components with known vulnerabilities, as defined by OWASP.

After completing this course, you will understand how to:

- Monitor applications for out of date components
- Triage and apply updates for known vulnerabilities
- Apply secure coding practices over the lifetime of an application

---

DES 231 – Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (12 mins)

In this course, you will learn how to mitigate the risks associated with insufficient logging and monitoring, as defined by OWASP.

After completing this course, you will understand how to:

- Ensure all login, access failures, and input validation failures are logged
- Implement sufficient user context to identify suspicious behavior
- Allow sufficient time so malicious accounts can be tracked for forensic analysis
- Apply best practices for secure application logging

DES 255 – Securing the IoT Update Process (30 mins)

Addressing updates across the Internet of Things (IoT) can be complicated due to the complex ecosystems of connected devices deployed across multiple environments. This course aims to educate learners to establish a secure, scalable update process for IoT devices.

After completing this course, you will be able to:

- Identify the risks of delivering IoT device updates
- Understand each phase in the IoT update process
- Determine considerations for the secure delivery of updates to the vehicle
- Securely design, develop, delivery, and install IoT update

DES 260 – Fundamentals of IoT Architecture & Design (30 mins)

This course focuses on topics related to architecting and designing a secure Internet of Things (IoT) system. Particular emphasis is placed on embedded IoT devices and their relationship with cloud services.

After completing this course, you will have a deep understanding of an IoT system, its components, and the security implications of various design choices.

Topics include:

- Elements to be reviewed and defined in the requirements phase
- Authorization considerations within the IoT device itself as well as connected components
- Designing a secure IoT architecture
- Authentication to validate the identity of users and devices
- Logical access controls to ensure users are granted appropriate levels of service
- Physical security concerns to protect access to IoT devices
- Monitor communications throughout the IoT system
- Secure communications between the various system components

DES 271 – OWASP M1: Mitigating Improper Platform Usage (12 mins)

In this course, you will learn how to mitigate the risks associated with Improper Platform Usage which might include Android intents, platform permissions, misuse of TouchID, the keychain, or some other security control that is part of the mobile operating system.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to improper platform usage
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 272 – OWASP M2: Mitigating Insecure Data Storage (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Data Storage which includes threat agents such as an adversary that has attained a lost/stolen mobile device; malware or another repackaged app acting on the adversary's behalf that executes on the mobile device.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insecure data storage
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 273 – OWASP M3: Mitigating Insecure Communication (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Communication which might include threat agents such as an adversary that shares local network (compromised or monitored Wi-Fi); carrier or network devices (routers, cell towers, proxy's, etc); or malware on your mobile device.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insecure communication
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 274 – OWASP M4: Mitigating Insecure Authentication (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Authentication which is typically exploited through automated attacks that use available or custom-built tools.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to Insecure Authentication
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 275 – OWASP M5: Mitigating Insufficient Cryptography (12 mins)

In this course, you will learn how to mitigate the risks associated with Insufficient Cryptography which includes threat agents such as anyone with physical access to data that has been encrypted improperly, or mobile malware acting on an adversary's behalf.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insufficient cryptography
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 276 – OWASP M6: Mitigating Insecure Authorization (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Authorization which allows an adversary to execute functionality they should not be entitled to using an authenticated but lower-privilege user of the mobile app.

After completing this course, you will be able to:

- Identify best practices for implementing secure authorization for Mobile Internet of Things
- How to mitigate the threat of Insecure Authorization
- Identify and mitigate Insecure Direct Object Reference (IDOR) vulnerabilities

---

DES 277 – OWASP M7: Mitigating Client Code Quality (12 mins)

In this course, you will learn how to mitigate the risks associated with poor code quality, including threat agents such as entities that can pass untrusted inputs to method calls made within mobile code.

After completing this course, you will be able to:

- Identify Uncontrolled Format String and Classic Buffer Overflow
- Recognize their potential impact
- Apply coding best practices to avoid them
- Find these weaknesses in your mobile application's source code
- Test your application to detect them

DES 278 – OWASP M8: Mitigating Code Tampering (12 mins)

In this course, you will learn how to mitigate the risks associated with code tampering. Typically, an attacker will exploit code modification via malicious forms of the apps hosted in third-party app stores. The attacker may also trick the user into installing the app via phishing attacks.

After completing this course, you will be able to:

- Identify code tampering vulnerabilities
- Defend against code tampering attacks

DES 279 – OWASP M9: Mitigating Reverse Engineering (12 mins)

In this course, you will learn how to mitigate risks associated with reverse engineering in which an attacker will typically download the targeted app from an app store and analyze it within their local environment using a suite of different tools.

After completing this course, you will be able to:

- Describe what kinds of knowledge reverse engineering may reveal to an attacker
- List mitigation techniques for reverse engineering

DES 280 – OWASP M10: Mitigating Extraneous Functionality (12 mins)

In this course, you will learn how to mitigate the risks associated with extraneous functionality. Typically, an attacker seeks to understand extraneous functionality within a mobile app in order to discover hidden functionality in backend systems. The attacker will typically exploit extraneous functionality directly from their own systems without any involvement by end-users.

After completing this course, you will be able to:

- Identify Extraneous Functionality
- Understand how an attacker might exploit this vulnerability in your software
- Mitigate exposure to this threat

DES 281 – OWASP IoT1: Mitigating Weak, Guessable or Hardcoded Passwords (12 mins)

In this course, you will learn how to mitigate the risks associated with the use of easily brute-forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

When you have completed this course, you will be able to:

- Identify best practices for implementing secure authentication for the Internet of Things
- Identify and mitigate password weaknesses in your applications

---

DES 282 – OWASP IoT2: Mitigating Insecure Network Services (12 mins)

In this course, you will learn how to mitigate the risks associated with unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.

After you have completed this course, you will be able to:

- Identify best practices to protect network services on IoT devices, including:
    - Only open necessary ports
    - Do not overexpose ports
    - Block unusual traffic
    - Mitigate DoS vulnerabilities
    - Mitigate memory corruption vulnerabilities|Disable outdated protocols

---

DES 283 – OWASP IoT3: Mitigating Insecure Ecosystem Interfaces (12 mins)

In this course, you will learn how to mitigate the risks associated with insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

After completing this course, you will be able to:

- Identify common threats to IoT web interfaces
- Apply best practices to mitigate these threats

DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

After you have completed this course, you will be able to:

- List the steps of a typical update process
- Describe how to protect update connections
- Explain how to protect the update server
- List the steps to securely sign and verify an update
- Evaluate whether Secure Boot is necessary for your device at this time
- Identify types of sensitive data that should not be included in updates
- Securely implement transport encryption for an Internet of Things (IoT) system

---

DES 285 – OWASP IoT5: Mitigating Use of Insecure or Outdated Components (12 mins)

In this course, you will learn how to mitigate the risks associated with the use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms and the use of third-party software or hardware components from a compromised supply chain.

After you have completed this course, you will be able to identify and mitigate threats posed by insecure and outdated components.

DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection (12 mins)

In this course, you will learn how to mitigate the risks associated with a user's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

After completing this course, you will learn to:

- Identify threats to personal information

- Identify ways to protect personal information

DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

After completing this course, you will be able to:

- Identify missing encryption
- Recognize the potential impact of this security defect
- Apply best practices to prevent insecure data transfer and storage

---

DES 288 – OWASP IoT8: Mitigating Lack of Device Management (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanism.

After completing this course, you will be able to:

- Monitor and Track Assets
- Monitor, Handle and Retain Information
- Monitor and Control System and Network Access

DES 289 – OWASP IoT9: Mitigating Insecure Default Settings (12 mins)

In this course, you will learn how to mitigate the risks associated with devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

After you have completed this course, you will be able to understand insecure default settings and their mitigation techniques.

DES 290 – OWASP IoT10 Mitigating Lack of Physical Hardening (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

After completing this course, you will be able to:

- Understand fail-safe defaults
- Use best practices for hardening

DES 306 – Creating a Secure Blockchain Network (20 mins)

While Blockchain technology continues to emerge for its ability to improve data security, speed up transactions and save costs, it comes with its advantages it comes with a wide array of challenges. Properly securing a blockchain network begins with the implementation of strong authentication and cryptography key vaulting mechanisms. This course provides learners with an understanding of the essential requirements for creating a secure blockchain network.

After completing this course you will be able to:

- Identify operational, legal and compliance requirements
- Create a blockchain threat model
- Create blockchain trust policies, access controls, and smart contracts
- Manage identity, access, entitlements, certificates, and keys
- Monitor, report, and manage incidents

DES 311 – Creating Secure Application Architecture (45 mins)

Architecting secure solutions is paramount to ensure developers do not incorporate insecure components, which could introduce hundreds of individual security vulnerabilities in the as-built system. This course covers a set of key security principles to improve the security of application architecture and design.

Topics include:

- Applying defense to harden applications and make them more difficult for intruders to breach
- Reducing the amount of damage an attacker can accomplish
- Compartmentalizing to reduce the impact of exploits
- Using centralized input and data validation to protect applications from malicious input
- Reducing the risk in error code paths

DES 312 – Protecting Cardholder Data (20 mins)

While cardholder data consists of any personally identifiable information (PII) associated with a person who has a credit or debit card, the PCI Secure Standards Council (PCI SSC) has specific requirements to protect cardholder data at all times. Despite common misconceptions, this also includes account numbers, expiration date, and/or service code as cardholder data. This course is designed to provide Information Systems Security Developers with the knowledge needed to minimize the storage of cardholder data and take necessary precautions to protect it in adherence to the PCI Software Security Framework and NIST 800-53 Guidelines.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Ensuring the software does not store sensitive authentication data after authorization, even if encrypted unless the software is intended only for use by issuers or organizations that support issuing services.
- Rendering the Primary Account Number (PAN) is unreadable anywhere it is stored.
- Guiding customers regarding the secure deletion of cardholder data after the expiration of the customer-defined retention period.

DSO 253 – DevSecOps in the AWS Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure AWS services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Implement inventory and configuration controls and services, including AWS Config, AWS CloudFormation, and Amazon Inspector
- Ensure Infrastructure Security using Amazon VPC, AWS WAF, Customer-controlled encryption and automatic encryption of all traffic
- Mitigate DDoS threats with Autoscaling, Amazon CloudFront and Amazon Route 53
- Encrypt data using AWS Key Management Services (KMS), Server-side encryption (SSE), AWS CloudHSM; and leverage EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift encryption features
- Meet Monitoring and Logging requirements using AWS CloudTrail and Amazon CloudWatch
- Use Identity and Access Controls to define, enforce, and manage user access policies with AWS Identity and Access Management (IAM), AWS Multi-Factor Authentication and AWS Directory Services
- Understand AWS policies for customer Penetration Testing

DSO 254 – DevSecOps in the Azure Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. Provides learners with an understanding of how to align and configure Azure services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Identify and manage the data, personnel, devices, systems, and facilities to meet the organization's business objectives and risk strategy
- Protect assets and associated facilities by using Access Control, limiting access to authorized users, processes, or devices, and to authorized activities and transactions

- Protect data-at-rest and data-in-transit by leveraging security services such as Azure Storage Service Encryption, Azure Backup Data Encryption, Azure SQL Transparent Data Encryption BitLocker, Azure VPN Gateway
- Detect anomalous activity in a timely manner and understand the potential impact of events by using Azure Security Center, Advanced Threat Analytics, Design and Implementation for Active Directory (DIAD), SIEM integration and Cloud App Security
- Ensure response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events

---

DSO 256 – DevSecOps in the Google Cloud Platform (COMING SOON) (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure Google Cloud Services to meet the NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.
Upon successful completion of this course, you will have the knowledge and skills to:

- Use Identity and Access Controls to define, enforce, and manage user access policies with Google Cloud Identity and Access Management (IAM)
- Develop strategies for integrating security into your DevOps pipeline
- Use different strategies for securing pipeline resources
- Understand different methods for protecting secrets used in deployment applications

---

DSO 302- Automated Security Testing (20 mins)

Modern application development, increasing speed-to-market requirements, and assuring application security have made automated security testing a top priority for many organizations. Automating Security Testing can be difficult and daunting, but incorporating into workflows can provide consistency, expedience, and ensure software quality. This course teaches learners to integrate the built-in strengths of DevOps within the security Testing process while adhering to security testing needs.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Understanding the importance of orchestrating secure system and service configuration
- Determining which types of automated tests should be performed at various stages of the software development lifecycle
- Creating policies that support simultaneous testing and building in keeping with DevSecOps secure software development
- Leveraging Information Security Continuous Monitoring (ISCM) tools to perform a broad range of tasks, including periodic security and vulnerability scans of all system components

---

DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)

APIs are a critical component of cloud computing, and modern development fueling the success of DevOps. This course enables learners to implement mechanisms to securely manage API requests through the use of API gateways in DevOps and serverless environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Deployment of secure API gateways through the implementation of core features such as to request and response collapsing API Transformation, and Protocol Translation for microservice-based applications
- Implement secure Identity and Access Management (IAM) across all services
- Provide certificate management, secrets management, and encryption services
- Leverage APIs to gather, synthesize and alert on security-relevant events as part of a comprehensive cybersecurity risk management program

---

DSO 306 – Implementing Infrastructure as Code (20 mins)

Used to automate infrastructure deployment processes, Implementing Infrastructure as Code comes with a unique set of challenges making it hard for organizations to maintain agility, control, and visibility. This course is designed to help developers leverage Infrastructure as Code to securely and effectively launch cloud environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Using tools in the development stage to help convert requirements into source code
- Leveraging the security features available in most integrated development environments (IDEs) for multiple programming language support
- Identify and mitigate the most common IaC vulnerabilities, including Weak Authentication Tokens, Disclosure of Authentication Credentials, Excessive Privileges or Capabilities, Misconfigured Network Filtering, and Missing Encryption

---

DSO 307 – Secure Secrets Management (20 mins)

As the need to protect critical data increases, organizations must focus efforts on improving processes used to manage essential information. This course is designed to ensure software development teams employ appropriate techniques to manage identities, privileges, and secrets securely.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Ensuring that approved cryptographic algorithms and methods are used for securing critical assets
- Aligning key-management processes and procedures with those recognized by industry-standards bodies
- Using Approved Random Number Generators| Providing strong entropy when Using Random Number Generator

---

ENG 114 – Essential Risk Assessment (15 mins)

This infrastructure security course provides essential guidance on information system risk assessment techniques. Individuals responsible for information systems, IT security, risk management, or oversight responsibilities will find this course valuable. It teaches how to define and manage the purpose, scope, roles, and coordination among organizational entities to help ensure appropriate risk assessment and compliance with applicable regulatory requirements.

Topics include:

- Security categorization
- Risk assessment
- Vulnerability scanning
- The system development lifecycle
- Security engineering principles
- Developer security testing and evaluation
- Development process, standards, and tools
- Developer security architecture and design
- Component authenticity

ENG 115 – Essential System & Information Integrity (15 mins)

This infrastructure security course provides essential guidance to program managers, system designers and developers on how to identify systems affected by software flaws, assess potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel.

Topics include:

- Flaw remediation
- Malicious code protection
- Information system monitoring
- Software, firmware, and information integrity
- Information input validation
- Error handling
- Information handling and retention
- Information output filtering
- Memory protection

ENG 116 – Essential Security Planning Policy & Procedures (15 mins)

This infrastructure security course provides training to individuals with information security implementation and operational responsibilities for developing and disseminating an organization-wide security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance mapping.

Topics include:

- Establishing rules of behavior
- Security concept of operations
- Personnel security policies and procedures
- Position risk designations
- Personnel screening
- Access agreements

ENG 117 – Essential Information Security Program Planning (15 mins)

This infrastructure security course provides essential guidance to individuals with information security implementation and operational responsibilities on how to build and communicate an information security program plan to facilitate compliance with applicable regulatory requirements.

Topics include:

- Identifying information security resources
- Performing an information system inventory
- Creating a critical infrastructure plan
- Risk management strategy
- Insider threat program
- Training and developing contacts with security groups and associations

---

ENG 120 – Essential Security Assessment & Authorization (15 mins)

This infrastructure security course provides guidance for developing and implementing personnel security policies and associated controls to help ensure appropriate screening, on-boarding, and off-boarding of staff.

Topics include:

- Position risk designation
- Personnel screening and termination
- Personnel transfer and access agreement

ENG 123 – Essential Security Engineering Principles (15 mins)

This infrastructure security course provides direction to program managers, system designers, developers, information security engineers, and systems integrators responsible for new information systems development or systems undergoing major upgrades.

Topics include:

- System development life cycle
- Developer security testing and evaluation
- Development process, standards, and tools
- Developer security architecture
- Design and component authenticity

ENG 124 – Essential Application Protection (15 mins)

This infrastructure security course imparts guidance to system designers and developers on implementing specific security controls at the software level to protect applications and comply with applicable regulatory requirements.

Topics include:

- Implementing defense-in-depth
- Separation of system and user functionality
- Securing components
- Validating input
- Encoding output

ENG 126 – Essential Security Maintenance Policies (15 mins)

This infrastructure security course offers guidance to individuals with information security implementation and operational responsibilities for developing system maintenance procedures and controls.

Topics include:

- Controlled maintenance
- Maintenance tools
- Non-local maintenance
- Timely maintenance

ENG 150 – Meeting Confidentiality, Integrity, and Availability (30 mins)

The CIA Triad – Confidentiality, Integrity, and Availability are the information security tenets used as a means for analyzing and improving the security of your application and its data. After completing this course, you will be able to understand and use confidentiality, integrity, and availability (CIA) as the three main tenets of information security.

ENG 191 – Introduction to the Microsoft SDL (25 mins)

This course introduces the industry-leading Microsoft Security Development Lifecycle (SDL) Optimization Model and how to implement it.

Topics include:

- Capability areas of the Microsoft SDL Optimization Model
- Maturity levels and how to reach them
- Optimization techniques to reduce risk

ENG 192- Implementing the Agile Microsoft SDL (20 mins)

The standard MS SDL process follows the traditional incremental waterfall model, while Agile methodologies are more iterative. This course focuses on the Agile variation of the SDL process and covers the following topics:

- How to map critical SDL security practices into every-sprint requirements, bucket or periodic requirements, and one-time requirements
- How to incorporate security education, tooling and automation, threat modeling, fuzz testing, handling bug-dense and at-risk code, exceptions, and the final security review into sprints

---

ENG 193 – Implementing the Microsoft SDL Optimization Model (12 mins)

This course describes the main phases of the Microsoft Security Development Lifecycle (SDL) process: Requirements, Design, Implementation, Verification, and Release, with a focus on security throughout.

After completing this course, you will have a solid understanding of the SDL process and the recommended/required tasks for each phase.

ENG 194 – Implementing Microsoft SDL Line of Business (20 mins)

This course describes the Microsoft Security Development Lifecycle for Line of Business (SDL-LOB), which focuses on the development of internal or business-facing applications.

Topics include:

- The five primary phases of the SDL: Requirements, Design, Implementation, Verification, and Release
- LOB-specific tasks, requirements and deliverables for each phase of the SDL
- How to integrate security-improving tasks at each level of risk
- Necessary skills to be effective

ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)

This course describes the features of the Microsoft SDL Threat Modeling tool, which complements the Microsoft SDL Threat Modeling process. While not required to perform threat modeling, using the tool facilitates the creation of threat models and helps enumerate threats using STRIDE.

Topics include:

- Creating accurate data flow diagrams (DFDs) in your threat model
- Identifying flaws in DFDs and analyzing it for potential threats
- Generating reports to export threats to issue tracking tools

---

ENG 205 – Fundamentals of Threat Modeling (45 mins)

This course describes how to take a question-driven approach to threat modeling to help identify security design problems early in development process.

After completing this course, you will be able to create a threat model for your application scenario and use it to refine your application's design and improve communication within the team.

ENG 212 – Implementing Secure Software Operations (20 mins)

All software activity involving critical assets must be tracked, and any methods that may expose sensitive data should also be tracked as defined by control objectives within the PCI Software Security Framework. Unfortunately, protecting the integrity of event datasets and analyzing records to detect attacks in real-time can be challenging. This course is designed to equip Information Systems Security Developers and Software Developers with the knowledge required to detect, respond to, and investigate attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet the Secure Software Operations requirements described in PCI's Secure Software Requirements and Assessment Procedures, including:

- Ensuring that all access attempts and usage of critical assets are tracked and traceable to a unique individual
- Facilitating the retention of detailed activity records either within the software itself or by supporting integration with other solutions such as centralized log servers, cloud-based logging solutions, or a back-end monitoring solution
- Ensuring that the software possesses the basic functionality to differentiate between normal and anomalous user behavior: such changes in post-deployment configurations or obvious automated-attack behaviors

---

ENG 251 – Risk Management Foundations (20 mins)

Risk management should be a foundational tool used to facilitate thoughtful and purposeful defense strategies. In today's environment, the most significant threats to systems come from purposeful attacks that are often disciplined, well organized, and well-funded.

This course aims to educate IT architects, Analysts, and DevOps Engineers to understand their responsibilities when protecting organizational assets.

Topics Include:

- Key Risk Management Concepts
- Common management techniques and strategies
- various risk assessment methods and risk control strategies

---

ENG 312 – How to Perform a Security Code Review (30 mins)

Application developers have a variety of tools at their disposal to identify flaws in their software. However, many of them cannot be used until late in the development lifecycle: dynamic analysis tools require a staging site and sample data, and some static analysis tools require a compiled build. In contrast, manual code reviews can begin at any time leveraging secure coding knowledge. Because manual security code reviews can be laborious if done inefficiently, this course focuses on time saving but effective techniques.

Topics include:

- How to organize and approach code reviews
- Prioritizing code segments to be reviewed
- Maximizing security resources

ENG 351 – Preparing the Risk Management Framework (20 mins)

Before any organization can adequately Implement the Risk Management Framework they must understand how to determine and apply appropriate security requirements. Preparation requires a disciplined and structured set of activities in order to execute the framework at appropriate risk management levels.

This course aims to provide Engineers, Software Architects, and Systems Analysts with context and priorities for managing security and privacy risk.

Topics Include:

- Identifying key Individuals and specification of roles and responsibilities in the risk management process
- Identifying risk tolerance and determining a particular strategy for risk management
- Conducting an organization-level risk assessment to ensure leadership is aligned
- Continuous monitoring to enable a rapid and effective response to changes in the risk landscape or changes in the effectiveness of controls

---

ENG 352 – Categorizing Systems and Information within the RMF (10 mins)

Security categorization provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system. This course provides learners with an understanding of how to categorize the system and the information using the NIST SP 800-37 Rev. 2 Risk Management Framework.

After completing this course you will be able to:

- Identify all information types based on the system boundary
- Categorize information (processed, stored, or transmitted) by the potential adverse impact that information being compromised as regards confidentiality, integrity or availability
- Ensure the security categorizations are consistent with roles, operating environment, connectivity, and intended use

---

ENG 353 – Selecting, Implementing and Assessing Controls within the RMF (20 mins)

Selecting the appropriate set of security controls helps to achieve organizational operations and objectives. This course provides learners with an understanding of how to select, implement and assess security controls using the NIST SP 800-37 Rev. 2 Risk Management Framework.

After completing this course you will be able to:

- Select and document the controls necessary to protect the information system and organization commensurate with the risk to the organization
- Implement the controls in the security and privacy plans for the system and organization
- Document the specific details of the control implementation in a baseline configuration
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements

---

ENG 354 – Authorizing and Monitoring System Controls within the RMF (20 mins)

Authorizing and monitoring security controls provides an understanding of security posture and provides an indication of whether or not cybersecurity controls are operating as intended. This course provides learners with an understanding of the Authorization and Monitoring steps of the NIST SP 800-37 Rev. 2 Risk Management Framework.

After completing this course you will be able to:

- Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk to operations, assets, and individuals is acceptable
- Report authorization decisions, significant vulnerabilities, and risks to organizational officials | Monitoring the system and the associated controls on an ongoing basis
- Document changes to the system and environment of operation
- Conduct risk assessments and impact analyses | Reporting the security and privacy posture of the system

---

SDT 311 – Testing for Integer Overflow or Wraparound (15 mins)

An integer overflow or wraparound may often be intended behavior; however, it can also introduce other weaknesses and security consequences. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-190 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Integer Overflow issues through code review
- Application of secure coding best practices to prevent these attacks
- Testing to detect Integer Overflow or Wraparound

SDT 312 – Testing for (Path Traversal) Improper Limitation of a Pathname to a Restricted Directory (15 mins)

Many file operations are intended to take placed within a restricted directory, however, the software does not properly neutralize special elements within a pathname which results in various security consequences. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-22 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding path traversal issues through code review
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 313 – Testing for (CSRF) Cross Site Request Forgery (15 mins)

Cross-Site Request Forgery (CSRF) occurs when a web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-352 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding CSRF issues through code review
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 314 – Testing for Unrestricted Upload of File with Dangerous Type (15 mins)

Unrestricted Upload of File with Dangerous Type vulnerabilities allows attackers to upload malicious code. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-434 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Unrestricted Upload vulnerabilities in an application source code
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 315 – Testing for Incorrect Permission Assignment for Critical Resource (15 mins)

The use of insecure settings for access permissions allows attackers to perform unauthorized access either to some part of the system or to an application-controlled resource. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-732 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability

- Techniques for finding Incorrect Permission Assignment for Critical
- Resource in an application source code
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 316- Testing for Use of Hard-Coded Credentials (15 mins)

Applications that use authentication need a method for storing credentials that is secure because when a hacker recovers credentials, they can use them to authenticate with the application or to access external services. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-798 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Hard-Coded credentials in source code
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 317 – Testing for Improper Control of Generation of Code (10 mins)

When user input can influence dynamically generated code to influence program flow or execute arbitrary code the attack is often referred to as code injection. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-94 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Understanding various forms of this attack and their similarities
- Techniques for finding Hard-Coded credentials in source code
- Application of mitigation techniques for limiting the impact
- Leveraging various tools used to test for code injection vulnerabilities

---

SDT 318 – Testing for Insufficiently Protected Credentials (10 mins)

Much of the security we rely upon at some point comes down to the passwords we use to authenticate an application. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-522 by the 2020 CWE Top 25.

Topics include:

- Understanding the applicability and impact of this weakness in depth
- Using appropriate security mechanism to protect credentials
- Applying methods of prevention, testing, and mitigation to defend against Insufficiently Protected Credentials

---

SDT 319 – Testing for Out-of-bounds Read (10 mins)

Out-of-bounds Read is a security defect that can allow attackers to read sensitive information from other memory locations or cause a crash. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-125 by the 2020 CWE Top 25.

Topics include:

- Identifying Out-of-bounds Read errors
- Recognizing the impact of this vulnerability
- Application of secure coding best practices
- Testing to detect errors

SDT 320 – Testing for Out-of-bounds Write (10 mins)

Out-of-bounds Write can result in corruption of data, a crash, or code execution. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-787 by the 2020 CWE Top 25.
Topics include:

- Identifying Out-of-bounds Write errors
- Recognizing the impact of this vulnerability
- Application of secure coding best practices
- Testing to detect errors

SDT 321 – Testing for Uncontrolled Resource Consumption (10 mins)

Uncontrolled Resource consumption occurs when software does not properly control the allocation and maintenance of limited resources such as memory, file system storage, database connection pool entries, and CPU. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-400 by the 2020 CWE Top 25.

Topics include:

- Identifying Uncontrolled Resource Consumption
- Recognizing the impact of this vulnerability
- Application of secure coding best practices
- Testing to detect this vulnerability

SDT 322 – Testing for Improper Privilege Management (10 mins)

Improper Privilege Management occurs when software does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-269 by the 2020 CWE Top 25.

Topics include:

- Identifying main threats that lead to abusing the privilege
- Recognizing the impact of this vulnerability
- Best practices for defending against unmanaged privileges
- Testing to detect Improper Privilege Management

SDT 324 – Testing for Improper Restriction of Operations within the Bounds of a Memory Buffer (10 mins)

Improper Restriction of Operations within the Bounds of a Memory Buffer allows attackers to execute arbitrary code, alter the intended control flow, read sensitive information, or cause a system to crash. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-119 by the 2020 CWE Top 25.

Topics include:

- Identifying Out of Range Memory Access errors
- Recognizing the impact of this vulnerability
- Applying preventative measures to avoid this weakness
- Common code mitigation strategies
- Using a multi-pronged approach to test for Improper Restriction of Operations with the Bounds of a Memory Buffer

---

SDT 325 – Testing for NULL Pointer Dereference (10 mins)

NULL pointer dereferences issues can occur through a number of flaws, including race conditions and simple programming omissions. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-476 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Defending Against NULL Pointer Dereference
- Best practices for preventing NULL Pointer Dereference
- Testing techniques for spotting NULL Pointer Dereference
- Mitigation strategies for this weakness

SDT 326 – Testing for Use After Free (10 mins)

The use of previously-freed memory can have any number of adverse consequences, but these errors have two common and sometimes overlapping causes. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-416 by the 2020 CWE Top 25.

Topics include:

- Identification of Use After Free Errors
- Recognizing the impact of this vulnerability
- Defending against Use After Free weaknesses
- Methods of Prevention
- Testing techniques for spotting Use After Free
- Secure coding best practices for mitigating this vulnerability

---

TST 101 – Fundamentals of Security Testing (20 mins)

This course introduces security testing concepts and processes that will help testers/QA teams analyze an application from a security perspective to conduct more effective security testing.

Topics include:

- Classes of security vulnerabilities and testing approaches that target them
- Manual and automated test techniques
- Identifying common security issues
- Threat modeling, approaches and how they apply to the design phase of the SDLC
- Vulnerability scanning, penetration testing, static analysis, and code review

---

TST 205 – Performing Vulnerability Scans (45 mins)

Performing vulnerability scans is a necessary first step to evaluating the security of an organization's network and helping protect organizational data and assets; this includes assessing, mitigating, and reporting on any security vulnerabilities that exist in an organization's systems and software.

Topic includes:

- Enumerating Platforms, Software Flaws, and improper configurations
- Formatting Checklists and test procedures
- Measuring vulnerability impact
- Analyzing vulnerability scan reports and results from security control assessments

---

Software Development (DEV)

COD 110 – Fundamentals of Secure Mobile Development (45 mins)

This course introduces developers to mobile environment threats and risks and presents secure programming principles to mitigate them.

Topics include:

- Common threats to mobile applications: client-side injection, sensitive data handling, network transition, application patching, web-based attacks, phishing, third-party code, location security and privacy and denial of service
- Defensive coding techniques: input validation, output encoding, least privilege, code signing, data protection at rest and in transit, avoiding client side validation, and using platform security capabilities as they apply in mobile environments
- Threat modeling of mobile applications

COD 152 – Fundamentals of Secure Cloud Development (20 mins)

This course introduces developers to the common risks associated with Cloud applications and secure coding best practices to mitigate them.

Topics include:

- Security features of the different series models (IaaS, PaaS, and SaaS)
- How to identify common vulnerabilities and code defensively to avoid them
- Common threats to cloud applications: unauthorized account access, insecure APIs, shared technology, data leakage, and account hijacking
- Complying with regulatory requirements
- The unique security challenges of "Big Data"
- How to apply the Microsoft SDL (https://siwpestage.wpengine.com/course-category/standard/ms-sdl/) to cloud applications

---

COD 160 -Fundamentals of Secure Embedded Software Development (45 mins)

Embedded devices tend to be linked to other devices via a wide array of technologies and often susceptible to targeted attacks. This course identifies security issues inherent to embedded devices and their deployment environments. You will also learn about the appropriate constraint of functionality from a security standpoint, and techniques to prevent common vulnerabilities.

Topics include:

- Techniques to identify system security and performance requirements
- Developing appropriate security architecture
- Selecting the correct mitigations
- How to develop policies that can ensure the secure operation of your system

---

COD 170 – Identifying Threats to Mainframe COBOL Applications & Data (20 mins)

This secure coding course covers the most common security issues that affect the confidentiality, integrity and availability of COBOL programs on mainframes. These include SQL Injection, Command Injection, Integer Overflow, Weak Cryptography, Unencrypted Communications and Race Conditions.

COD 201 – Secure C Encrypted Network Communications (15 mins)

This course explores secure communications using Transport Layer Security (TLS) and best practices for implementing these within C and C++ applications.

Topics include:

- Key principles of TLS
- Libraries and interfaces for implementing the TLS protocol
- TLS security considerations
- Alternatives to TLS

COD 202 – Secure C Runtime Protection (15 mins)

This secure coding course covers common run-time protection technologies that can be used to protect an application from attack.

Topics include:

- Run-time protection technologies and how to apply them to your applications
- Stack security cookies, Address Space Layout Randomization (ASLR), and No-eXecute (NX)
- Limitations of run-time protection technologies

COD 206 – Creating Secure C++ Code (15 mins)

This secure coding course highlights the most useful security features for avoiding memory corruption vulnerabilities in C++.

Additional topics include:

- Standard containers, bounds-checking functions, smart pointers, and standard concurrency features
- How to use object-oriented programming features to define and manipulate data in terms of objects, use range-based loops and native regular expressions

---

COD 207 – Communication Security in C++ (15 mins)

This secure coding course focuses on how to protect data in transit using encryption libraries and strong TLS ciphers in C++.

Topics include:

- Important issues about public key certificates including signing and verification
- Using well-trusted encryption libraries and strong TLS cipher suites to protect data in transit
- Protect and verify the integrity of public key certificates

---

COD 214 – Creating Secure GO Applications (30 mins)

As organizations continue to migrate to cloud infrastructures; development teams are finding themselves leveraging GO as a tool of choice. Lightweight and quick to compile due to generous libraries and abstractions that make it easier to program concurrent and distributed (read: cloud) applications it offers a slew of benefits from Static compilation with no dependencies, a strong standard library, a full development environment, and the ability to build for multiple architectures with no minimal hassle.

This course will provide software developers and DevOps Engineers with working knowledge of fundamental concepts and advanced features of the GO programming language.

Topics Include:

- Identifying and preventing SQL injection attacks
- Understanding cross-site scripting
- Properly configuring browser cookies
- Understanding and preventing session hijacking attacks
- Knowing how to avoid cross-site request forgery vulnerabilities
- Understanding the difference between symmetric and asymmetric cryptography
- Implementing transport layer security
- Working with hashes and key derivation functions

*Indicates that the course is still in production and subject to change

---

COD 216 – Leveraging .NET Framework Code Access Security (CAS) (30 mins)

This course explores the foundation of .NET, the CLR's native security infrastructure (Code Access Security), and the ASP.NET security infrastructure.

Topics include:

- Differences between managed and unmanaged code
- Access control functions in Windows
- Code Access Security (CAS) functions in .NET
- Interactions between Windows access control and CAS
- Key aspects of ASP.NET security and understand the Level 2 Security Transparency Model

---

COD 217 – Mitigating .NET Security Threats (45 mins)

With a primary focus on .NET secure error handling and secure logging, this course describes secure coding techniques to avoid information disclosure and other vulnerabilities.

Topics include:

- Avoiding dangerous patterns when using CAS
- Avoiding common .NET security pitfalls
- Ensuring application fail safely

COD 219 – Creating Secure Code: SAP ABAP Foundations (90 mins)

This secure coding course presents best practices and techniques for secure SAP application development using Java and ABAP.

Topics include:

- Key application security principles, vulnerabilities and mitigations
- Validating input in SAP applications
- Protecting data using encryption
- Conducting security code analysis and code reviews

COD 241 – Creating Secure Oracle DB Applications (45 mins)

This secure coding course introduces database application developers to key industry best practices for data security.

Topics include:

- Secure query construction
- Secure communication and storage
- Creating safe stored procedures to prevent SQL Injection
- How to secure data at rest and data in transit using Oracle Database features

---

COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)

This secure coding course explores protecting sensitive data and ensuring the integrity of applications running on the Microsoft SQL Server Engine and Azure SQL Database.

Topics include:

- The security function of roles in controlling user and principal access to SQL Server securables
- Exercising fine-grained controls that adhere to the Principle of Least Privilege
- Leveraging the security features of Microsoft's Azure SQL Database to protect sensitive data and ensure the integrity of your applications

---

COD 246 – PCI DSS 3: Protecting Stored Cardholder Data (15 mins)

In this course, you will learn how to use the CWE-311 guidelines to identify, test and mitigate for missing encryption of sensitive data. Coverage includes techniques for spotting missing encryption through code review and testing. Secure coding best practices are included, as well as descriptions of technology-specific weaknesses as appropriate. This course requires basic knowledge of client-server applications, web applications, the Software Development Life Cycle, cryptography, and the STRIDE model.

COD 247 – PCI DSS 4: Encrypting Transmission of Cardholder Data (15 mins)

In this course, you will learn about the risks of insecure communications and how to use the CWE guidelines, specifically the OWASP Top Ten, to mitigate these risks. Coverage includes techniques for spotting missing encryption and using Transport Layer Security (TLS).

COD 248 – PCI DSS 6: Develop and Maintain Secure Systems and Applications (15 mins)

In this course, you will learn to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities. Coverage will be aligned with the CWE SANS Top 25 and OWASP 2017 Top 10 vulnerability frameworks.

COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software, system components, and custom software. The software should be tested regularly to ensure security controls continue to reflect a changing environment.

In this course, you will learn how to ensure critical data can only be accessed by authorized personnel and develop an understanding of systems and processes that must be in place to limit access based on a need to know and according to job responsibilities. Additionally, you will learn how to test security controls and ensure they continue to reflect a changing environment.

COD 251 – Defending AJAX-Enabled Web Applications (25 mins)

This course introduces fundamentals of how to defend AJAX-enabled Web applications, including the difference between regular and AJAX-enabled web applications, AJAX security checks against challenges, and common attacks against AJAX-enabled applications.

Topics include:

- Architectural differences between regular web applications and AJAX-enabled applications
- Identifying threats to AJAX applications: cross-site scripting (XSS), cross-site request forgery (CSRF), and injection attacks
- Implementing countermeasures against attacks: protecting client resources, validating input, protecting web services requests, preventing request forgeries, and securing data access.

COD 253 – Creating Secure AWS Cloud Applications (45 mins)

This course examines the security vulnerabilities, threats, and mitigations for AWS cloud computing services and provides best practices for securing Web applications by leveraging AWS platform security features.

Topics include:

- AWS security features: Key Management Service (KMS), Hardware Security Module (HSM), Identity and Access Management (IAM), and CloudWatch
- How to leverage security features built into Common Amazon Cloud services such as Simple Storage Service (S3), Elastic Compute Cloud (Amazon EC2), Elastic Block Store (EBS), Amazon Glacier, Relational Database Service (RDS), DynamoDB, Elastic MapReduce (EMR), and Amazon Machine Images (AMI)

COD 254 – Creating Secure Azure Applications (45 mins)

This course examines key Azure security platforms and services that you can use to improve the security of your applications.

Topics include:

- Security vulnerabilities, threats, and mitigations for Azure cloud computing services
- How to identify common security threats to cloud-based applications
- Secure coding best practices to mitigate threats
- How to leverage built-in Azure features for an extra layer of defense

---

COD 255 – Creating Secure Code: Web API Foundations (20 mins)

This secure coding course introduces the fundamentals of secure web services development.

Topics include:

- Common web services threats that put your application at risk
- Impact of web services attacks
- Secure development best practices to protect web services

COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Ruby on Rails. After completing this course, you will be able to identify and mitigate injection vulnerabilities, such as SQL injection and cross-site scripting, build strong session management into your Rails applications, and prevent other common vulnerabilities, such as cross-site request forgery and direct object access.

Topics include:

- How to identify and mitigate injection vulnerabilities: SQL Injection (SQLi) and cross-site scripting (XSS)
- How to build strong session management into your rails applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF) and direct object access

---

COD 257 – Creating Secure Python Web Applications (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Python. After completing this course, you will be able to understand various types of injection vulnerabilities, including SQL injection and cross-site scripting. You will also be able to understand how to build strong session management into your Python web applications and how to prevent common vulnerabilities, such as cross-site request forgery, direct object access, and others.

Finally, you will be able to recognize file system threats to web applications, including vulnerabilities with path traversal, temporary files, and insecure client redirects.

Topics include:

- Types of Injection Vulnerabilities including SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- File system threats to web applications including vulnerabilities with path traversal, temporary files, and insecure client redirects
- How to build strong session management into your python web applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF), direct object access, and others

---

COD 258 – Creating Secure PHP Web Applications (30 mins)

In this course, you will learn important concepts for secure PHP scripting. After completing this course, you will be able to use quotation marks correctly, discuss techniques for handling return codes and exceptions, canonicalize paths to identify the correct files, identify dangerous functions to avoid, apply techniques for preventing or mitigating different injection vulnerabilities, recognize that regular expressions must be handled carefully to avoid DoS attacks, and describe techniques to protect sensitive data in transit.

Topics covered:

- Key defensive coding principles such as proper session management, error handling, authentication, authorization, data storage, and use of encryption
- Avoiding and mitigating vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), File Inclusion, Command Injection, Cross-Site Request Forgery (CSRF) and Null Byte attacks

---

COD 259 – Node.js Threats & Vulnerabilities (30 mins)

In this secure coding course, you will learn about system configuration, injection attacks, session management, package management, and the AngularJS framework, all within the context of Node.js security.

Topics include:

- Best practices for Node.js server and system configuration
- Types of injection attacks and mitigation techniques
- Proper settings for session cookie security
- Mitigating cross-site request forgery (CSRF) attacks
- Leveraging popular static analysis tools for Node.js
- Understand why templates and expressions are vulnerable to injection
- Methods, services, elements, and parameters that should not be used with untrusted data
- Best practices for loading templates

COD 261 – Threats to Scripts (30 mins)

In this secure coding course, you will learn about the impact of incorrect script development or lax security measures.

Topics include:

- Outcomes of vulnerable scripts
- Common scripting vulnerabilities such as SQL Injection (SQLi)
- Security issues related to permissions and privileges
- Impact of different types of resource

COD 262 – Fundamentals of Shell and Interpreted Language Security (30 mins)

In this secure coding course, you will learn about how shell scripting languages compare with more modern interpreted languages with respect to security features, and defensive coding techniques, and dealing with common differences between platforms that can alter script behavior.

Topics incude:

- Information security principles including least privilege and defense in depth
- The importance of data validation and how to validate using input, array indices, and environment variables
- Using file system operations safely to protect
- Preventing or mitigating cached secret disclosure
- The importance of up-to-date communication security techniques
- Operating system (OS) system portability issues

COD 263 – Secure Bash Scripting (15 mins)

In this secure coding course, you will learn about the importance of error and exception handling in shell scripts and interpreted languages such as Perl, Python, Bash and Ruby.

Topics covered:

- Techniques for handling errors and exceptions in shell scripts and interpreted languages
- Common syntax pitfalls and dangerous functions to avoid
- Techniques for preventing/mitigating different vulnerabilities including different types of injection

---

COD 264 – Secure Perl Scripting (15 mins)

Perceived as being difficult to fix in comparison to other programming languages Perl is commonly known as “the duct-tape of the Internet.” This general-purpose programming language is currently being used for a wide range of tasks as it takes the best features from other languages.

In this course, you will learn about best practices for secure scripting in Perl, features of Perl’s taint mode, handling errors in Perl, protecting files, preventing format string and injection vulnerabilities, using regular expressions carefully, and protecting sensitive data in transit with Transport Layer Security (TLS).

COD 265 – Secure Python Scripting (15 mins)

In this secure coding course, you will learn important concepts for secure Python scripting including techniques for error and exception handling.

Topics Covered:

- Avoiding uncontrolled format string vulnerabilities
- Defending against Regular Expression Denial of Service (DoS) attacks
- Protecting sensitive data in transit
- Techniques for preventing/mitigating different vulnerabilities including different types of injection

---

COD 266 – Secure Ruby Scripting (15 mins)

In this secure coding course, you will learn important concepts for secure Ruby scripting, techniques for preventing/mitigating different vulnerabilities including different types of injection, and protecting sensitive data in transit.

Topics covered:

- Validating command-line parameters
- Using quotation marks correctly
- Using unmask to set default file permissions
- Protecting files and canonicalizing paths
- Defending against Regular Expression Denial of Service (DoS) attacks

---

COD 267 – Securing Python Microservices (30 mins)

Microservices have become widely popular, replacing complicated XML-based schemas and service-oriented architectures (SOA) because of the ability to create separate, well-defined, individual components within a system. By leveraging python microservices, complex applications can be broken down into these components to ease further development and deployment.

This course will provide cloud developers, python developers, and software architects with a working knowledge of possible attacks, how to secure interaction between services and an understanding of how to implement basic principles to ensure the security of python microservices.

Topics Include:

- Techniques for handling return codes and exceptions
- Canonicalizing paths to identify the correct files
- Identifying dangerous functions
- Applying techniques for mitigating injection vulnerabilities
- How to securely handle regular expressions
- How to protect sensitive data

COD 270 – Creating Secure COBOL & Mainframe Applications (25 mins)

This secure coding course covers countermeasures for security vulnerabilities on mainframe systems such as input validation, parameterized APIs, strong cryptography, and memory management issues.

Topics include:

- Identifying vulnerabilities and threats to mainframe applications and data
- Mitigating SQL injection threats using safe prepared statements and parameterized APIs
- Validating all input
- Using exec* functions instead of system functions to mitigate the risk of command injection
- Using key derivation functions to protect stored password
- Encrypting sensitive data at rest using AES-256
- Protecting sensitive data in transit with TLS
- Preventing deadlocks by using the ENQ and DEQ commands
- Avoiding manual memory management in order to prevent buffer overflow conditions

---

COD 281 – Java Security Model (20 mins)

In this secure coding course, you will learn about Java's policy-driven security model and how to leverage it to build more secure applications.

Topics include:

- Java security model components
- Functions of the Java security manager and access controller
- Java security policies and the Java security policy files

COD 283 – Java Cryptography (45 mins)

This secure coding course explores the key concepts of public key cryptography and teaches you how to use the Java keytool command-line utility for creating and managing keys and keystores.

Topics include:

- How public and private key pairs work together to encrypt and decrypt data for secure transfer and to create and verify digital signature
- Generating secure encryption keys and identifying related issues such as pseudo random number generators (PRNGs), key derivation functions, and initialization vectors
- Selecting an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode

---

COD 284 – Secure Java Coding (30 mins)

In this course, you will learn about secure Java coding practices, including techniques for avoiding Denial of Service (DoS) and regular expression DoS attacks, and guidelines for secure error handling and logging. You will also become familiar with the dangers of unreleased resources, null references, and XML external entity (XXE) attacks

Topics include:

- Denial of Service and designing your application to handle or avoid such situations
- Guidelines for secure error handling and logging
- Identify the dangers of unreleased resources, null references, and XML external entity attacks

---

COD 285 – Developing Secure Angular Applications (30 mins)

Widely adopted amongst the software development community because of the versatility it provides, securing angular applications comes with a steep learning curve. While component-based architecture is one of the key benefits of using angular, managing components can be complicated. This course is designed to develop the skills required to design, build, and maintain secure Angular applications following software assurance best practices.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure Angular.js compliance requirements, including:

- Securing AngularJS templates to help mitigate threats from expression Injection and dynamically loading templates from untrusted sources
- Ensuring that both the server and the client cooperate to eliminate these threats and potential security issues that need to be blocked
- Implementing Content Security Policies and secure routing

COD 286 – Creating Secure React User Interfaces (10 mins)

This JavaScript library has become a popular choice in the market because of its ability to help solve web development challenges. The framework makes it painless to create interactive user interfaces, design simple view, and reactively update to changes. This course is designed to develop the skills required to securely build user interfaces using multiple components and implement best practices to avoid common attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure React.js User Interfaces compliance requirements, including:

- Creating secure React components
- Avoiding vulnerable third-party React component libraries
- Preventing React component injection attacks
- Using and serializing JSON

COD 301 – Secure C Buffer Overflow Mitigations (45 mins)

This course focuses on C-language buffers. Upon completion of this course you will learn good memory management techniques and coding best practices to help you avoid buffer & integer overflows, format string vulnerabilities, and race conditions.

Topics include:

- Mitigating buffer overflows and race conditions
- Preventing memory management, format string, injection and integer overflow vulnerabilities
- Protecting data in memory

COD 302 -Secure C Memory Management (20 mins)

This secure coding course focuses on memory manipulation and allocation techniques for C-language software development.

Topics include:

- Key concepts of dynamic memory management
  Common mistakes that lead to Out of Range Memory Access
- Best practices to mitigate memory management vulnerabilities
- How to ensure that “freed” or “deleted” data in memory is no longer accessible

---

COD 303 – Common C Vulnerabilities & Attacks (20 mins)

In this secure coding course, you will review common C application vulnerabilities, how they manifest in code; as well as techniques and libraries that you can use to mitigate the risk of attack.

After completing this course, you will be able to mitigate risk from the following vulnerabilities:

- Format string attacks
- Integer overflows
- Path Traversal issues
- Command injection
- SQL injection

COD 307 – Protecting Data in C++ (25 mins)

This secure coding course presents key concepts of public key cryptography, the risks of improper encryption, and defensive coding techniques to protect sensitive data.

Topics include:

- Generating strong encryption keys and identifying related issues such as pseudo random number generators (PRNGs), key derivation algorithms, and initialization vectors
- Selecting an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode
- Common libraries that support symmetric cryptography
- How public and private key pairs work together both to encrypt and decrypt data for secure transfer and to create and verify digital signatures
- Best practices to mitigate memory exposure vulnerabilities

COD 308 – Common ASP.NET MVC Vulnerabilities and Attacks (45 mins)

This course provides an overview of code security issues that affect ASP.NET MVC applications. You will also understand how other vulnerabilities can be mitigated with careful and complete input validation.

After completing this course, you will be able to understand model validation and its strengths and weaknesses, understand and prevent unique attacks, such as under-posting and over-posting, and implement protective measures against SQL injection, cross-site scripting, cross-site request forgery, and malicious URL redirects.

COD 309 – Securing ASP.NET MVC Applications (30 mins)

This course teaches the fundamentals of authentication and authorization in ASP.NET Web API, and the roles they play in the OWIN pipeline.

After completing this course, you will understand:

- Web API pipeline and where each component sits on that path
- Authentication and authorization filters and the role of each in your Web API application
- Different authentication options and how to implement them in your application
- The importance of secure communication and the use of Transport Layer Security (TLS) to create secure data exchange tunnels.

COD 315 – Preventing Vulnerabilities in iOS Code in Swift (20 mins)

In this secure coding course, you will learn how to code defensively to prevent iOS security vulnerabilities.

Topics Include:

- Mitigation approaches and Implementing Secure Coding Best Practices
- How to leverage iOS and Swift security services to mitigate threats
- Pros and Cons of Biometrics such as Touch ID and Face ID

COD 316 – Creating Secure iOS Code in Objective C (30 mins)

This secure coding course describes techniques for creating secure iOS applications.

Topics include:

- Common vulnerabilities such as exposure of authentication credentials, sensitive data, and other secrets; custom URL scheme abuse; and XML eXternal Entity (XXE) Injection
- Techniques for mitigating vulnerabilities including protecting data at rest with the Data Protection and Common Crypto APIs, mitigating sensitive data exposure in background snapshots, preventing custom URL scheme abuse, and mitigating XXE Injection

---

COD 317 – Protecting Data on iOS in Swift (20 mins)

In this secure coding course, you will learn how to code defensively to protect data on iOS

Topics Include:

- Protecting data in transit and at Rest
- App Transport Security (ATS and default settings
- Use of Valid Certificates and Certificate Pinning
- Using URL Loading System to establish Network Connections
- iOS Cryptography Framework and Data Protection Features

COD 318 – Protecting Data on Android in Java (20 mins)

In this secure coding course, you will learn how to protect data on Android applications using Java.

Topics include:

- Protecting Data in transit using Transport Layer Security (TLS)
- Protecting Data at rest using Symmetric Key Encryption
- Using Android KeyStor to Protect Data
- Dangers of External Storage on Android

COD 319 – Preventing Vulnerabilities in Android Code in Java (20 mins)

In this secure coding course, you will learn to meet Android security quality standards using Java.

Topics include:

- Restricting access to Interprocess Communications and shared data
- Applying the Principle of Least Privilege and deferring permissions
- Avoiding disclosure of sensitive data
- Reducing attack vectors for Cross-Site Scripting (XSS)
- Keeping all libraries and dependencies current

COD 321 – Protecting C# from Integer Overflows & Canonicalization (30 mins)

This secure coding course describes methods that will produce secure C# applications.

Topics include:

- Common security vulnerabilities such as Canonicalization Issues and Integer Overflows
- Unique features of C# and the .NET Framework that can be used to mitigate them
- Understand where and when canonicalization issues and integer overflows are likely to occur
- Avoiding common pitfalls

COD 322 – Protecting C# from SQL Injection (8 mins)

This secure coding course presents SQL Injection vulnerabilities and the features of the .NET Framework that can be used to mitigate them.

Topics include:

- Where and when SQL injection is likely to occur
- Avoiding common pitfalls when defending against SQL injection
- Defense-in-Depth Strategies and best practices for mitigating injection vulnerabilities

---

COD 323 – Using Encryption with C# (20 mins)

This secure coding course describes techniques to protect data both in transit and at rest in C# applications using strong cryptography.

Topics include:

- How to protect data using the Data Protection API (DPAPI)
- Avoiding common cryptographic pitfalls
- Protecting sensitive data in transit
- Alternatives to Transport Layer Security (TLS)

COD 324 – Protecting C# from XML Injection (8 mins)

This secure coding course presents XML Injection vulnerabilities and the features of the .NET Framework that can be used to mitigate them.

Topics include:

- Where and when XML injection is likely to occur
- Avoiding common pitfalls when defending against XML injection
- Defense-in-Depth Strategies and best practices for mitigating injection vulnerabilities

---

COD 352 – Creating Secure JavaScript and jQuery Code (45 mins)

In this secure coding course, you will learn about common client-side vulnerabilities and threats to jQuery applications, and techniques for mitigating them.

Additional topics include:

- How to implement new HTML5 security features to secure jQuery applications
- Best practices to secure local storage and implement Transport Layer Security

---

COD 361 – HTML5 Secure Threats (15 mins)

In this secure coding course, you will learn about security risks introduced by HTML5.

Additional topics include:

- Threats to HTML5 such as cross-site scripting (XSS), cross-site request forgery (CSRF), clickjacking, and threats to user privacy
- Secure coding techniques to mitigating HTML5 threats

COD 362 – HTML5 Built in Security Features (20 mins)

This secure coding course describes important HTML5 security features and how to leverage them to produce more robust applications.

Topics include:

- Implementing Same-Origin Policy, Content Security Policy, Cross-Origin Resource Sharing, and IFrame Sandboxing
- Understanding the limitations of Same-Origin Policy
- Employing best practices to avoid common attacks on HTML5 applications

---

COD 363- Securing HTML5 Data (20 mins)

In this course, you will learn about new features that raise security issues in HTML5 forms, security issues surrounding local data storage, best practices for HTML5 connectivity with the WebSocket API and Server-ent Events, and best practices for the Web Workers, History, Geolocation, and Drag and Drop APIs.

COD 364 – Securing HTML5 Connectivity (20 mins)

In this course, you will learn about best practices for securing connections used by applications that leverage HTML5.

COD 366 – Creating Secure Kotlin Applications (20 mins)

As a prime option for building android applications because of its interoperability with java code, maintainability, reliability, and ability to boost team efficiency, Kotlin is being widely adopted but comes with its own set of challenges as does any technology. This course is designed to ensure learners avoid common mistakes and pitfalls as they leverage vital features and build secure mobile applications using this general-purpose programming language.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Enforcing secure communication by safeguarding the data that you exchange between your app and other apps, or between your app and a website, thereby improving your app's stability and protecting the data that you send and receive.
- Using intents to defer permissions
- Storing all private user data within the device's internal storage (which is sandboxed per app)
- Ensuring the device deletes all files when the user uninstalls an app

---

COD 370- Testing for OWASP 2017: Injection (15 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A1:2017 family of injection security vulnerabilities, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for various injection flaws and mitigation measures to protect against them.

COD 371 – Testing for OWASP 2017: Broken Authentication (12 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A2:2017 security vulnerability broken authentication, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for broken authentication flaws and mitigation measures to protect against them.

COD 372 – Testing for OWASP 2017: Sensitive Data Exposure (12 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A3:2017 security vulnerability sensitive data exposure, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for sensitive data exposure flaws and mitigation measures to protect against them.

COD 373 – Testing for OWASP 2017: XML External Entities (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A4:2017 security vulnerability XML external entities, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for XML external entities flaws and mitigation measures to protect against them.

COD 374 – Testing for OWASP 2017: Broken Access Control (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A5:2017 security vulnerability Broken Access Control, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for broken access control flaws and mitigation measures to protect against them.

COD 375 – Testing for OWASP 2017: Security Misconfiguration (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A6:2017 vulnerability security misconfiguration, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for security misconfiguration flaws and mitigation measures to protect against them.

COD 376 – Testing for OWASP 2017: Cross Site Scripting (XSS) (15 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A7:2017 Cross-Site Scripting (XSS) misconfiguration, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for XSS flaws and mitigation measures to protect against them.

COD 377 – Testing for OWASP 2017: Insecure Deserialization (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A8:2017 Insecure Deserialization vulnerability, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for insecure deserialization flaws and mitigation measures to protect against them.

COD 378 – Testing for OWASP 2017: Use of Components with Known Vulnerabilities (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A9:2017 security vulnerability Using Components with Known Vulnerabilities, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for flaws related to known insecure components and mitigation measures to protect against them.

COD 379 – Testing for OWASP 2017: Insufficient Logging & Monitoring (10 mins)

This course explains how testers and developers can determine if their web applications are vulnerable to the A10:2017 Insufficient Logging and Monitoring vulnerability, as identified by the Open Web Application Security Project (OWASP).

After completing this course, you will understand how to test your application for insufficient logging and monitoring flaws and mitigation measures to protect against them.

COD 380 – Preventing SQL Injection in Java (8 mins)

This secure coding course describes ways to remediate and prevent SQL Injection (SQLi) vulnerabilities in your Java application.

Topics Include:

- Identifying data types that require encryption
- Best practices for encryption methods
- Avoiding common encryption errors

COD 381 – Preventing Path Traversal Attacks in Java (8 mins)

This secure coding course describes ways to mitigate security risks from Path Traversal Attacks in your Java application.

Topics Include:

- Identifying Path Traversal Attacks and understanding how they work
- Normalizing, canonicalizing, and validating file paths
- Implementing countermeasures to prevent Path Traversal Attacks

---

COD 382 – Protecting Data in Java (30 mins)

This course discusses protecting data at rest and in transit in Java applications. Several code examples are provided to illustrate key concepts.

After completing this course, you will be able to protect data at rest appropriate cryptographic techniques and protect data in transit with appropriate cryptographic techniques.

COD 383 – Protecting Java Backend Services (30 mins)

Backends are designed for applications that need faster performance, large amounts of addressable memory, and continuous or long-running background processes. The versatility of Java enables developers to design and deliver the right business solutions however their efficiency requires distinctive experiencer and great expertise.

This course aims to provide software developers and DevOps Engineers with the next level understanding of best practices for developing back end frameworks using Java while developing skills necessary to handle user input and build secure systems.

Topics Include:

- The Function of OAuth2 and JWT
- How to leverage the JAAS API
- The advantages of the Spring Security framework
- Validating Length Before Applying RegEx
- Protecting Sensitive Data in Transit Using TLS
- How to identify and protect against SQLi, HQLi, XXE, CSRF, and RegEx DoS attacks

---

COD 384 – Protecting Java from Information Disclosure (8 mins)

This secure coding course describes ways to identify and prevent Information disclosure in your Java application.

Topics Include:

- Identifying common Java information disclosure issues
- Protecting Java applications through improved error messaging
- Best practices for preventing information disclosure
- Audit error handling for information disclosure vulnerability

---

COD 385 – Preventing Race Conditions in Java Code (8 mins)

This secure coding course describes ways to identify and prevent race conditions in your Java application.

Topics Include:

- Common Java race condition issues
- Security risks introduced by race conditions
- Secure protection of temp files
- Best practices for preventing race condition issues

COD 386 – Preventing Integer Overflows in Java Code (8 mins)

This secure coding course describes ways to write code to identify and mitigate risks from integer overflows.

Topics Include:

- Common Integer Overflow security risks and prevention methods
- Precondition Testing, Upcasting, and BigInteger Objects
- Google Guava

- Common Integer Overflow Pitfalls

DES 202 – Cryptographic Suite Services: Encoding, Encrypting & Hashing (45 mins)

This course presents an overview of the fundamental services provided by cryptographic suites, namely encoding, encrypting, and hashing.

Topics include:

- Encoding and decoding
- Encryption and decryption
- The difference between encoding and encryption
- The value and application of hashing
- Where, when, and how to use crypto

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s): K0018: Knowledge of encryption algorithms.

DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)

This course introduces three important elements of cryptographic systems: random number generation, algorithms and keys.

Topics include:

- The critical role of randomness in cryptography
- Common algorithms to perform cryptographic manipulation of information
- Types and roles of cryptographic keys
- The key management problem
- Common types of digital certificates and its creation process
- Components and roles of a public key infrastructure
- Weaknesses in the digital certificate trust mode
- Mechanisms to manage and distribute cryptographic keys

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 204 – Role of Cryptography in Application Development (15 mins)

This course introduces cryptography and how cryptography can help secure software applications and data. It also provides an overview of common uses of cryptography.

Topics include:

- Identifying relevant cryptographic technologies
- Knowing common “data-in-motion” crypto options and the strengths/weaknesses of each
- Applying common “data-at-rest” crypto options and the strengths/weaknesses of each

---

DES 205 – Message Integrity Cryptographic Functions (45 mins)

This course explains how encrypting and signing a message works, how message authentication codes work, and why a digital signature is superior to a cryptographic hash for validating software integrity.

Topics include:

- Message integrity function is its value
- The difference between a message authentication code and a digital signature
- How a digital signature works
- Encrypting and signing messages
- Message authentication codes

- Digital signature vs. a cryptographic hash for validating software integrity

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 212 – Architecture Risk Analysis & Remediation (30 mins)

This course defines concepts, methods, and techniques for analyzing the architecture and design of a software system for security flaws. Special attention is given to analysis of security issues in existing applications; however, the principles and techniques are applicable to systems under development. Techniques include accurately capturing application architecture, threat modeling with attack trees, attack pattern analysis, and enumeration of trust boundaries.

Topics include:

- How to assess design components for security flaws
- The use and value of threat modeling and attack surface analysis
- Techniques to remove architecture weak spots and avoid vulnerability propagation

---

DES 222 – Applying OWASP 2017: Mitigating Injection (12 mins)

In this course, you will learn how to mitigate the risks associated with injection, as defined by OWASP.

After completing this course, you will understand how to:

- Keep data separate from commands and queries
- Implement multi-factor authentication
- Require weak-password checks
- Limit login attempts

DES 223 – Applying OWASP 2017: Mitigating Broken Authentication (12 mins)

In this course, you will learn how to mitigate the risks associated with broken authentication, as defined by OWASP.
After completing this course, you will understand how to:

- Use secure coding best practices to confirm user identity
- Implement strong authentication mechanisms
- Protect user sessions and session data

DES 224 – Applying OWASP 2017: Mitigating Sensitive Data Exposure (12 mins)

In this course, you will learn how to mitigate the risks associated with sensitive data exposure, as defined by OWASP.

After completing this course, you will understand how to:

- Enforce the use of up-to-date and strong standards-based crypto algorithms
- Properly store passwords using strong adaptive and salted hashing functions
- Encrypt data in transit with secure protocols

DES 225 – Applying OWASP 2017: Mitigating XML External Entities (12 mins)

In this course, you will learn how to mitigate the risks associated with XML External Entities (XXE), as defined by OWASP.

After completing this course, you will understand how to:

- Apply secure coding practices to avoid serialization of sensitive data
- Patch all XML processors and libraries
- Implement server-side input validation

DES 226 – Applying OWASP 2017: Mitigating Broken Access Control (12 mins)

In this course, you will learn how to mitigate the risks associated with broken access control, as defined by OWASP.

After completing this course, you will understand how to:

- Implement access control policies
- Assess the effectiveness of current access controls
- Employ secure coding practices to ensure users cannot act outside intended permissions

---

DES 227 – Applying OWASP 2017: Mitigating Security Misconfiguration (12 mins)

In this course, you will learn how to mitigate the risks associated with security misconfiguration, as defined by OWASP.

After completing this course, you will understand how to:

- Segment application architecture
- Implement a concerted, repeatable application security configuration process
- Code defensively to avoid misconfiguration problems in deployment

---

DES 228 – Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (12 mins)

In this course, you will learn how to mitigate the risks associated with Cross-Site Scripting (XSS), as defined by OWASP.

After completing this course, you will understand how to:

- Leverage secure frameworks
- Implement secure coding practices to avoid XSS attacks
- Escape untrusted HTTP requests
- Apply context-sensitive encoding to separate untrusted data from active browser content

---

DES 229 – Applying OWASP 2017: Mitigating Insecure Deserialization (12 mins)

In this course, you will learn how to mitigate the risks associated with insecure deserialization, as defined by OWASP.

After completing this course, you will understand how to:

- Implement integrity checks such as digital signatures
- Apply secure coding practices for serialized objects
- Enforce strict type constraints
- Effectively restrict network connectivity

DES 230 – Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (12 mins)

In this course, you will learn how to mitigate the risks associated with using components with known vulnerabilities, as defined by OWASP.

After completing this course, you will understand how to:

- Monitor applications for out of date components
- Triage and apply updates for known vulnerabilities
- Apply secure coding practices over the lifetime of an application

---

DES 231 – Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (12 mins)

In this course, you will learn how to mitigate the risks associated with insufficient logging and monitoring, as defined by OWASP.

After completing this course, you will understand how to:

- Ensure all login, access failures, and input validation failures are logged
- Implement sufficient user context to identify suspicious behavior
- Allow sufficient time so malicious accounts can be tracked for forensic analysis

- Apply best practices for secure application logging

DES 255 – Securing the IoT Update Process (30 mins)

Addressing updates across the Internet of Things (IoT) can be complicated due to the complex ecosystems of connected devices deployed across multiple environments. This course aims to educate learners to establish a secure, scalable update process for IoT devices.

After completing this course, you will be able to:

- Identify the risks of delivering IoT device updates
- Understand each phase in the IoT update process
- Determine considerations for the secure delivery of updates to the vehicle
- Securely design, develop, delivery, and install IoT update

DES 271 – OWASP M1: Mitigating Improper Platform Usage (12 mins)

In this course, you will learn how to mitigate the risks associated with Improper Platform Usage which might include Android intents, platform permissions, misuse of TouchID, the keychain, or some other security control that is part of the mobile operating system.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to improper platform usage
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 272 – OWASP M2: Mitigating Insecure Data Storage (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Data Storage which includes threat agents such as an adversary that has attained a lost/stolen mobile device; malware or another repackaged app acting on the adversary's behalf that executes on the mobile device.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insecure data storage
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 273 – OWASP M3: Mitigating Insecure Communication (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Communication which might include threat agents such as an adversary that shares local network (compromised or monitored Wi-Fi); carrier or network devices (routers, cell towers, proxy's, etc); or malware on your mobile device.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insecure communication
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 274 – OWASP M4: Mitigating Insecure Authentication (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Authentication which is typically exploited through automated attacks that use available or custom-built tools.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to Insecure Authentication
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 275 – OWASP M5: Mitigating Insufficient Cryptography (12 mins)

In this course, you will learn how to mitigate the risks associated with Insufficient Cryptography which includes threat agents such as anyone with physical access to data that has been encrypted improperly, or mobile malware acting on an adversary's behalf.

After completing this course, you will be able to:

- Identify the most common security flaws in mobile apps related to insufficient cryptography
- Understand how an attacker might exploit such vulnerabilities in your software
- Eliminate or mitigate exposure to these common security threats

---

DES 276 – OWASP M6: Mitigating Insecure Authorization (12 mins)

In this course, you will learn how to mitigate the risks associated with Insecure Authorization which allows an adversary to execute functionality they should not be entitled to using an authenticated but lower-privilege user of the mobile app.

After completing this course, you will be able to:

- Identify best practices for implementing secure authorization for Mobile Internet of Things
- How to mitigate the threat of Insecure Authorization
- Identify and mitigate Insecure Direct Object Reference (IDOR) vulnerabilities

---

DES 277 – OWASP M7: Mitigating Client Code Quality (12 mins)

In this course, you will learn how to mitigate the risks associated with poor code quality, including threat agents such as entities that can pass untrusted inputs to method calls made within mobile code.

After completing this course, you will be able to:

- Identify Uncontrolled Format String and Classic Buffer Overflow
- Recognize their potential impact
- Apply coding best practices to avoid them
- Find these weaknesses in your mobile application's source code
- Test your application to detect them

DES 278 – OWASP M8: Mitigating Code Tampering (12 mins)

In this course, you will learn how to mitigate the risks associated with code tampering. Typically, an attacker will exploit code modification via malicious forms of the apps hosted in third-party app stores. The attacker may also trick the user into installing the app via phishing attacks.

After completing this course, you will be able to:

- Identify code tampering vulnerabilities
- Defend against code tampering attacks

DES 279 – OWASP M9: Mitigating Reverse Engineering (12 mins)

In this course, you will learn how to mitigate risks associated with reverse engineering in which an attacker will typically download the targeted app from an app store and analyze it within their local environment using a suite of different tools.

After completing this course, you will be able to:

- Describe what kinds of knowledge reverse engineering may reveal to an attacker
- List mitigation techniques for reverse engineering

DES 280 – OWASP M10: Mitigating Extraneous Functionality (12 mins)

In this course, you will learn how to mitigate the risks associated with extraneous functionality. Typically, an attacker seeks to understand extraneous functionality within a mobile app in order to discover hidden functionality in backend systems. The attacker will typically exploit extraneous functionality directly from their own systems without any involvement by end-users.

After completing this course, you will be able to:

- Identify Extraneous Functionality
- Understand how an attacker might exploit this vulnerability in your software
- Mitigate exposure to this threat

DES 281 – OWASP IoT1: Mitigating Weak, Guessable or Hardcoded Passwords (12 mins)

In this course, you will learn how to mitigate the risks associated with the use of easily brute-forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

When you have completed this course, you will be able to:

- Identify best practices for implementing secure authentication for the Internet of Things
- Identify and mitigate password weaknesses in your applications

---

DES 282 – OWASP IoT2: Mitigating Insecure Network Services (12 mins)

In this course, you will learn how to mitigate the risks associated with unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.

After you have completed this course, you will be able to:

- Identify best practices to protect network services on IoT devices, including:
    - Only open necessary ports
    - Do not overexpose ports
    - Block unusual traffic
    - Mitigate DoS vulnerabilities
    - Mitigate memory corruption vulnerabilities|Disable outdated protocols

---

DES 283 – OWASP IoT3: Mitigating Insecure Ecosystem Interfaces (12 mins)

In this course, you will learn how to mitigate the risks associated with insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

After completing this course, you will be able to:

- Identify common threats to IoT web interfaces
- Apply best practices to mitigate these threats

DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

After you have completed this course, you will be able to:

- List the steps of a typical update process
- Describe how to protect update connections
- Explain how to protect the update server
- List the steps to securely sign and verify an update
- Evaluate whether Secure Boot is necessary for your device at this time
- Identify types of sensitive data that should not be included in updates
- Securely implement transport encryption for an Internet of Things (IoT) system

---

DES 285 – OWASP IoT5: Mitigating Use of Insecure or Outdated Components (12 mins)

In this course, you will learn how to mitigate the risks associated with the use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms and the use of third-party software or hardware components from a compromised supply chain.

After you have completed this course, you will be able to identify and mitigate threats posed by insecure and outdated components.

DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection (12 mins)

In this course, you will learn how to mitigate the risks associated with a user's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

After completing this course, you will learn to:

- Identify threats to personal information
- Identify ways to protect personal information

DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

After completing this course, you will be able to:

- Identify missing encryption
- Recognize the potential impact of this security defect
- Apply best practices to prevent insecure data transfer and storage

---

DES 288 – OWASP IoT8: Mitigating Lack of Device Management (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of ability to securely update the device. This includes lack of firmware validation on a device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanism.

After completing this course, you will be able to:

- Monitor and Track Assets
- Monitor, Handle and Retain Information
- Monitor and Control System and Network Access

DES 289 – OWASP IoT9: Mitigating Insecure Default Settings (12 mins)

In this course, you will learn how to mitigate the risks associated with devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

After you have completed this course, you will be able to understand insecure default settings and their mitigation techniques.

DES 290 – OWASP IoT10 Mitigating Lack of Physical Hardening (12 mins)

In this course, you will learn how to mitigate the risks associated with a lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

After completing this course, you will be able to:

- Understand fail-safe defaults
- Use best practices for hardening

DES 311 – Creating Secure Application Architecture (45 mins)

Architecting secure solutions is paramount to ensure developers do not incorporate insecure components, which could introduce hundreds of individual security vulnerabilities in the as-built system. This course covers a set of key security principles to improve the security of application architecture and design.

Topics include:

- Applying defense to harden applications and make them more difficult for intruders to breach
- Reducing the amount of damage an attacker can accomplish
- Compartmentalizing to reduce the impact of exploits
- Using centralized input and data validation to protect applications from malicious input
- Reducing the risk in error code paths

DSO 253 – DevSecOps in the AWS Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure AWS services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Implement inventory and configuration controls and services, including AWS Config, AWS CloudFormation, and Amazon Inspector
- Ensure Infrastructure Security using Amazon VPC, AWS WAF, Customer-controlled encryption and automatic encryption of all traffic
- Mitigate DDoS threats with Autoscaling, Amazon CloudFront and Amazon Route 53
- Encrypt data using AWS Key Management Services (KMS), Server-side encryption (SSE), AWS CloudHSM; and leverage EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift encryption features
- Meet Monitoring and Logging requirements using AWS CloudTrail and Amazon CloudWatch
- Use Identity and Access Controls to define, enforce, and manage user access policies with AWS Identity and Access Management (IAM), AWS Multi-Factor Authentication and AWS Directory Services
- Understand AWS policies for customer Penetration Testing

DSO 254 – DevSecOps in the Azure Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. Provides learners with an understanding of how to align and configure Azure services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Identify and manage the data, personnel, devices, systems, and facilities to meet the organization's business objectives and risk strategy
- Protect assets and associated facilities by using Access Control, limiting access to authorized users, processes, or devices, and to authorized activities and transactions
- Protect data-at-rest and data-in-transit by leveraging security services such as Azure Storage Service Encryption, Azure Backup Data Encryption, Azure SQL Transparent Data Encryption BitLocker, Azure VPN Gateway
- Detect anomalous activity in a timely manner and understand the potential impact of events by using Azure Security Center, Advanced Threat Analytics, Design and Implementation for Active Directory (DIAD), SIEM integration and Cloud App Security
- Ensure response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events

---

DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)

APIs are a critical component of cloud computing, and modern development fueling the success of DevOps. This course enables learners to implement mechanisms to securely manage API requests through the use of API gateways in DevOps and serverless environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Deployment of secure API gateways through the implementation of core features such as to request and response collapsing API Transformation, and Protocol Translation for microservice-based applications
- Implement secure Identity and Access Management (IAM) across all services
- Provide certificate management, secrets management, and encryption services
- Leverage APIs to gather, synthesize and alert on security-relevant events as part of a comprehensive cybersecurity risk management program

---

DSO 306 – Implementing Infrastructure as Code (20 mins)

Used to automate infrastructure deployment processes, Implementing Infrastructure as Code comes with a unique set of challenges making it hard for organizations to maintain agility, control, and visibility. This course is designed to help developers leverage Infrastructure as Code to securely and effectively launch cloud environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Using tools in the development stage to help convert requirements into source code
- Leveraging the security features available in most integrated development environments (IDEs) for multiple programming language support
- Identify and mitigate the most common IaC vulnerabilities, including Weak Authentication Tokens, Disclosure of Authentication Credentials, Excessive Privileges or Capabilities, Misconfigured Network Filtering, and Missing Encryption

---

ENG 123 – Essential Security Engineering Principles (15 mins)

This infrastructure security course provides direction to program managers, system designers, developers, information security engineers, and systems integrators responsible for new information systems development or systems undergoing major upgrades.

Topics include:

- System development life cycle
- Developer security testing and evaluation
- Development process, standards, and tools
- Developer security architecture
- Design and component authenticity

ENG 124 – Essential Application Protection (15 mins)

This infrastructure security course imparts guidance to system designers and developers on implementing specific security controls at the software level to protect applications and comply with applicable regulatory requirements.

Topics include:

- Implementing defense-in-depth
- Separation of system and user functionality
- Securing components
- Validating input
- Encoding output

ENG 191 – Introduction to the Microsoft SDL (25 mins)

This course introduces the industry-leading Microsoft Security Development Lifecycle (SDL) Optimization Model and how to implement it.

Topics include:

- Capability areas of the Microsoft SDL Optimization Model
- Maturity levels and how to reach them
- Optimization techniques to reduce risk

ENG 192- Implementing the Agile Microsoft SDL (20 mins)

The standard MS SDL process follows the traditional incremental waterfall model, while Agile methodologies are more iterative. This course focuses on the Agile variation of the SDL process and covers the following topics:

- How to map critical SDL security practices into every-sprint requirements, bucket or periodic requirements, and one-time requirements
- How to incorporate security education, tooling and automation, threat modeling, fuzz testing, handling bug-dense and at-risk code, exceptions, and the final security review into sprints

---

ENG 193 – Implementing the Microsoft SDL Optimization Model (12 mins)

This course describes the main phases of the Microsoft Security Development Lifecycle (SDL) process: Requirements, Design, Implementation, Verification, and Release, with a focus on security throughout.

After completing this course, you will have a solid understanding of the SDL process and the recommended/required tasks for each phase.

ENG 194 – Implementing Microsoft SDL Line of Business (20 mins)

This course describes the Microsoft Security Development Lifecycle for Line of Business (SDL-LOB), which focuses on the development of internal or business-facing applications.

Topics include:

- The five primary phases of the SDL: Requirements, Design, Implementation, Verification, and Release
- LOB-specific tasks, requirements and deliverables for each phase of the SDL
- How to integrate security-improving tasks at each level of risk
- Necessary skills to be effective

ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)

This course describes the features of the Microsoft SDL Threat Modeling tool, which complements the Microsoft SDL Threat Modeling process. While not required to perform threat modeling, using the tool facilitates the creation of threat models and helps enumerate threats using STRIDE.

Topics include:

- Creating accurate data flow diagrams (DFDs) in your threat model
- Identifying flaws in DFDs and analyzing it for potential threats
- Generating reports to export threats to issue tracking tools

---

ENG 205 – Fundamentals of Threat Modeling (45 mins)

This course describes how to take a question-driven approach to threat modeling to help identify security design problems early in development process.

After completing this course, you will be able to create a threat model for your application scenario and use it to refine your application's design and improve communication within the team.

ENG 212 – Implementing Secure Software Operations (20 mins)

All software activity involving critical assets must be tracked, and any methods that may expose sensitive data should also be tracked as defined by control objectives within the PCI Software Security Framework. Unfortunately, protecting the integrity of event datasets and analyzing records to detect attacks in real-time can be challenging. This course is designed to equip Information Systems Security Developers and Software Developers with the knowledge required to detect, respond to, and investigate attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet the Secure Software Operations requirements described in PCI's Secure Software Requirements and Assessment Procedures, including:

- Ensuring that all access attempts and usage of critical assets are tracked and traceable to a unique individual
- Facilitating the retention of detailed activity records either within the software itself or by supporting integration with other solutions such as centralized log servers, cloud-based logging solutions, or a back-end monitoring solution

- Ensuring that the software possesses the basic functionality to differentiate between normal and anomalous user behavior: such changes in post-deployment configurations or obvious automated-attack behaviors

---

ENG 312 – How to Perform a Security Code Review (30 mins)

Application developers have a variety of tools at their disposal to identify flaws in their software. However, many of them cannot be used until late in the development lifecycle: dynamic analysis tools require a staging site and sample data, and some static analysis tools require a compiled build. In contrast, manual code reviews can begin at any time leveraging secure coding knowledge. Because manual security code reviews can be laborious if done inefficiently, this course focuses on time saving but effective techniques.

Topics include:

- How to organize and approach code reviews
- Prioritizing code segments to be reviewed
- Maximizing security resources

SDT 311 – Testing for Integer Overflow or Wraparound (15 mins)

An integer overflow or wraparound may often be intended behavior; however, it can also introduce other weaknesses and security consequences. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-190 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Integer Overflow issues through code review
- Application of secure coding best practices to prevent these attacks
- Testing to detect Integer Overflow or Wraparound

SDT 312 – Testing for (Path Traversal) Improper Limitation of a Pathname to a Restricted Directory (15 mins)

Many file operations are intended to take placed within a restricted directory, however, the software does not properly neutralize special elements within a pathname which results in various security consequences. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-22 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding path traversal issues through code review
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 313 – Testing for (CSRF) Cross Site Request Forgery (15 mins)

Cross-Site Request Forgery (CSRF) occurs when a web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-352 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding CSRF issues through code review
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 314 – Testing for Unrestricted Upload of File with Dangerous Type (15 mins)

Unrestricted Upload of File with Dangerous Type vulnerabilities allows attackers to upload malicious code. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-434 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Unrestricted Upload vulnerabilities in an application source code
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 315 – Testing for Incorrect Permission Assignment for Critical Resource (15 mins)

The use of insecure settings for access permissions allows attackers to perform unauthorized access either to some part of the system or to an application-controlled resource. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-732 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Incorrect Permission Assignment for Critical
- Resource in an application source code
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 316- Testing for Use of Hard-Coded Credentials (15 mins)

Applications that use authentication need a method for storing credentials that is secure because when a hacker recovers credentials, they can use them to authenticate with the application or to access external services. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-798 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Techniques for finding Hard-Coded credentials in source code
- Application of secure coding best practices to prevent these attacks
- Testing to detect this security weakness

SDT 317 – Testing for Improper Control of Generation of Code (10 mins)

When user input can influence dynamically generated code to influence program flow or execute arbitrary code the attack is often referred to as code injection. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-94 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Understanding various forms of this attack and their similarities
- Techniques for finding Hard-Coded credentials in source code
- Application of mitigation techniques for limiting the impact
- Leveraging various tools used to test for code injection vulnerabilities

---

SDT 318 – Testing for Insufficiently Protected Credentials (10 mins)

Much of the security we rely upon at some point comes down to the passwords we use to authenticate an application. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-522 by the 2020 CWE Top 25.

Topics include:

- Understanding the applicability and impact of this weakness in depth
- Using appropriate security mechanism to protect credentials
- Applying methods of prevention, testing, and mitigation to defend against Insufficiently Protected Credentials

---

SDT 319 – Testing for Out-of-bounds Read (10 mins)

Out-of-bounds Read is a security defect that can allow attackers to read sensitive information from other memory locations or cause a crash. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-125 by the 2020 CWE Top 25.

Topics include:

- Identifying Out-of-bounds Read errors
- Recognizing the impact of this vulnerability
- Application of secure coding best practices
- Testing to detect errors

SDT 320 – Testing for Out-of-bounds Write (10 mins)

Out-of-bounds Write can result in corruption of data, a crash, or code execution. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-787 by the 2020 CWE Top 25.
Topics include:

- Identifying Out-of-bounds Write errors
- Recognizing the impact of this vulnerability
- Application of secure coding best practices
- Testing to detect errors

SDT 321 – Testing for Uncontrolled Resource Consumption (10 mins)

Uncontrolled Resource consumption occurs when software does not properly control the allocation and maintenance of limited resources such as memory, file system storage, database connection pool entries, and CPU. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-400 by the 2020 CWE Top 25.

Topics include:

- Identifying Uncontrolled Resource Consumption
- Recognizing the impact of this vulnerability
- Application of secure coding best practices
- Testing to detect this vulnerability

SDT 322 – Testing for Improper Privilege Management (10 mins)

Improper Privilege Management occurs when software does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-269 by the 2020 CWE Top 25.

Topics include:

- Identifying main threats that lead to abusing the privilege
- Recognizing the impact of this vulnerability
- Best practices for defending against unmanaged privileges
- Testing to detect Improper Privilege Management

SDT 324 – Testing for Improper Restriction of Operations within the Bounds of a Memory Buffer (10 mins)

Improper Restriction of Operations within the Bounds of a Memory Buffer allows attackers to execute arbitrary code, alter the intended control flow, read sensitive information, or cause a system to crash. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-119 by the 2020 CWE Top 25.

Topics include:

- Identifying Out of Range Memory Access errors
- Recognizing the impact of this vulnerability
- Applying preventative measures to avoid this weakness
- Common code mitigation strategies
- Using a multi-pronged approach to test for Improper Restriction of Operations with the Bounds of a Memory Buffer

SDT 325 – Testing for NULL Pointer Dereference (10 mins)

NULL pointer dereferences issues can occur through a number of flaws, including race conditions and simple programming omissions. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-476 by the 2020 CWE Top 25.

Topics include:

- Recognizing the impact of this vulnerability
- Defending Against NULL Pointer Dereference
- Best practices for preventing NULL Pointer Dereference
- Testing techniques for spotting NULL Pointer Dereference
- Mitigation strategies for this weakness

SDT 326 – Testing for Use After Free (10 mins)

The use of previously-freed memory can have any number of adverse consequences, but these errors have two common and sometimes overlapping causes. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-416 by the 2020 CWE Top 25.

Topics include:

- Identification of Use After Free Errors
- Recognizing the impact of this vulnerability
- Defending against Use After Free weaknesses
- Methods of Prevention
- Testing techniques for spotting Use After Free
- Secure coding best practices for mitigating this vulnerability

---

TST 101 – Fundamentals of Security Testing (20 mins)

This course introduces security testing concepts and processes that will help testers/QA teams analyze an application from a security perspective to conduct more effective security testing.

Topics include:

- Classes of security vulnerabilities and testing approaches that target them
- Manual and automated test techniques
- Identifying common security issues
- Threat modeling, approaches and how they apply to the design phase of the SDLC
- Vulnerability scanning, penetration testing, static analysis, and code review

---

Systems Administration (ADM)

COD 141 – Fundamentals of Database Security (30 mins)

In practice, the database represents the goal of many attackers, as this is where the information of value is maintained. However, the functional requirements and security testing often focus on the interaction between a software user and the application, while the handling of data is assumed to be secure.

This course describes how to apply authentication and access control to your database and provides an understanding of database privileges and limiting data access. Coverage also includes techniques for protecting the database and methods for securely concealing specific data while providing an introduction to cloud databases and database encryption.

COD 252 – Securing Google Platform Applications & Data (COMING SOON) (25 mins)

Google Cloud Platform adoption provides many organizations with the agility and scalability needed to transform their business but lack of awareness surrounding best security practices and control implementation increases the risk of a security breach. This course provides the knowledge and skills to implement and leverage GCP security features, manage secrets, and protect applications and data

against common threats.

Topics Include:

- Google Cloud Platform security features
- Creating, managing, and protecting secrets
- Common security threats
- Google Cloud monitoring and auditing facilities.

COD 287 – Java Application Server Hardening (20 mins)

This secure operations and maintenance course introduce best practices for server hardening.

Topics Include:

- Minimizing unnecessary privileges and functionality
- Being current with dependencies and server software
- Protecting connections and data in transit

DES 210 – Hardening Linux/Unix Systems (30 mins)

Hardening is a critical step in ensuring security and diligence as it reduces the chances of attack, but this requires the use of appropriate methodologies. In today's connected world securing an operating system has become increasingly sophisticated as computing ecosystems increase in complexity. This course provides learners with an understanding of best practices for hardening Linux and Unix systems.

After completing this course you will be able to:

- Upgrade your kernel
- Disable root cron jobs
- Enforce strict firewall rules
- Disable unnecessary services
- Check for backdoors and rootkits
- Check listening ports
- Monitor and manage logs using IDS

DES 214 – Securing Infrastructure Architecture (UPDATED) (30 mins)

This course is designed for Network Operations Specialists and aligns with the NICE requirements for the secure planning, implementation, and operation of network services and systems, including hardware and virtual environments.

Coverage includes:

- Security Principles
- Network Topologies
- Demilitarized Zones
- Routers, Switches, Bridges, and Firewalls
- Wireless Access Points
- Transmission Media
- Network Authentication
- Server Configuration

DES 215 – Defending Infrastructure (UPDATED) (30 mins)

This course is designed for the System Administrator role and aligns with the NICE requirements for system administration on specialized cyber defense applications and systems (e.g, antivirus, audit, and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.

DSO 303 – Automating Security Updates (20 mins)

Essential to keeping systems secure, reducing risk, introducing new or enhanced features, or improving compatibility, software updating can be challenging and resource-intensive. Automating this process eliminates routine tasks and frees up administrative time. This course introduces automation procedures for systems administration to effectively and efficiently manage IT software in adherence to functional and security requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Employ automated mechanisms to implement changes to the current system baseline and deploy the updated baseline across the installed base
- Review system changes to determine whether unauthorized changes have occurred
- Remove previous versions of software or firmware components after installing updated versions
- Ensure that security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures

---

DSO 305 – Automating CI/CD Pipeline Compliance (20 mins)

The adoption of cloud infrastructure and DevOps requires consistent integration of security to achieve a reliable lifecycle of continuous deployment. Integrating compliance into the CI/CD Pipeline requires a coordinated effort by everyone involved in the development pipeline. This course enables learners to automate the implementation of security tasks across the CI/CD pipeline in adherence to compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Automate scanning and reporting tasks to ensure privacy policies, applicable laws, regulations, and service-level agreements are reviewed and documented for compliance regulations
- Identify and document controls owned by outside parties
- Configure change monitors to identify changes to organizational systems and environments of operation that may affect security and privacy risk
- Verify that all control objectives are met, and all key controls are designed and operating effectively

---

ENG 110 – Essential Account Management Security (15 mins)

This infrastructure security course provides essential guidance on implementing specific account management security controls at the hardware and software level to facilitate compliance with applicable regulatory requirements.

Topics include:

- How to define and control network access
- Creating a separation of duties policy
- Building and managing segregation of resources strategies
- Monitoring system access
- Using digital certificates for authentication

ENG 111 – Essential Session Management Security (15 mins)

This infrastructure security course provides guidance to system designers and developers on how to implement session management controls at the software level. These techniques enhance security of web applications and facilitates compliance with applicable regulatory requirements.

Topics include:

- Securing session identifiers
- Implementing Transport Layer Security (TLS) so sensitive data is always transmitted over secure channels
- Ensuring client browsers send cookies over HTTPS connections

---

ENG 112 – Essential Access Control for Mobile Devices (15 mins)

This infrastructure security course teaches designers and developers how to implement software-level access controls on mobile devices to mitigate threats, protect privacy, and comply with applicable regulatory requirements.

Topics include:

- Identifying threats to mobile devices
- The importance of protecting user privacy and confidentiality
- Methods for encrypting data at rest and data in transit
- Implementing application code signing to ensure software integrity

---

ENG 113 – Essential Secure Configuration Management (15 mins)

This infrastructure security course trains program managers, system designers, and developers on proper security practices for defining and implementing IT system configuration management.

Topics include:

- Key configuration practices and configuration change control
- Security impact analysis
- Access restrictions for change
- Principle of least functionality
- Information system component inventory

ENG 119 – Essential Security Audit & Accountability (15 mins)

This infrastructure security course trains information system owners, system administrators, and information system security officers on how to build and communicate effective audit policies and controls.

Topics include:

- Documenting security audits
- Implementing audit controls
- Using audit tools
- Generating audit reports

ENG 121 – Essential Identification & Authentication (15 mins)

This infrastructure security course teaches those responsible for information security how to develop identification and authentication policy and controls. The course spans personnel, devices, and information systems.

Topics include:

- Identification and authentication of users inside and outside your organization
- Device identification and authentication
- Identifier management
- Authenticator management and feedback
- Cryptographic module authentication
- Service identification and authentication
- Adaptive identification and authentication
- Processes for re-authentication

ENG 122 – Essential Physical & Environmental Protection (15 mins)

This infrastructure security course educates those responsible for developing physical and environmental protection policies how to create effective controls and comply with applicable regulatory requirements.

Topics include:

- Physical access authorizations and control
- Access control for transmission medium and output devices
- Monitoring physical access
- Information leakage, asset monitoring and tracking

ENG 125 – Essential Data Protection (15 mins)

This infrastructure security course delivers training to personnel in information systems, information security, systems design, software development, and IT operations on essential data security techniques. Focus is primarily on cryptographic controls at the information systems level and compliance with applicable regulatory requirements.

Topics include:

- Asymmetric key algorithms
- Using hash functions to protect data integrity
- Proper password storage for authentication purposes
- Encrypting file transfers and downloads
- Adding salt values before hashing
- Using Certificate Authorities

ENG 127 – Essential Media Protection (15 mins)

This infrastructure security course describes the development and dissemination of an organization-wide information media protection policy that addresses scope, roles, responsibilities, and coordination among organizational entities to facilitate compliance with applicable regulatory requirements.

Topics include:

- Best practices for media protection
- Controls for marking, storage, and transport of media
- Media sanitization and downgrading

SDT 323 – Improper Input Validation (10 mins)

Input validation is used to check potentially dangerous inputs but when software does not validate this input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This course introduces ways to identify and mitigate this security weakness, referenced as CWE-20 by the 2020 CWE Top 25.

Topics include:

- Identifying malicious input
- Recognizing the impact of this vulnerability
- Strategies for defending against Improper Input Validation
- Testing for Improper Input Validation weaknesses

Systems Analysis (ANA)

COD 287 – Java Application Server Hardening (20 mins)

This secure operations and maintenance course introduce best practices for server hardening.

Topics Include:

- Minimizing unnecessary privileges and functionality
- Being current with dependencies and server software
- Protecting connections and data in transit

DES 206 – Meeting Cloud Governance and Compliance Requirements (15 mins)

The adoption of cloud services involves various roles making it difficult to govern the selection and brokering of cloud services while adhering to policies and procedures. This course is designed to ensure privacy and security teams may effectively and efficiently adopt cloud computing in support of strategic and business goals.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Creating Policies, Procedures, Standards, and Controls that meet all regulatory and legal requirements, industry standards, and technical controls such as encryption.
- Establishing, deploy and assess a compliance baseline that determines targets
- Handling sensitive data, including how to identify and classify data, define data retention periods, and comply with data storage requirements.
- Prepare for compliance auditing and Reporting

DES 210 – Hardening Linux/Unix Systems (30 mins)

Hardening is a critical step in ensuring security and diligence as it reduces the chances of attack, but this requires the use of appropriate methodologies. In today's connected world securing an operating system has become increasingly sophisticated as computing ecosystems increase in complexity. This course provides learners with an understanding of best practices for hardening Linux and Unix systems.

After completing this course you will be able to:

- Upgrade your kernel
- Disable root cron jobs
- Enforce strict firewall rules
- Disable unnecessary services
- Check for backdoors and rootkits
- Check listening ports
- Monitor and manage logs using IDS

DES 215 – Defending Infrastructure (UPDATED) (30 mins)

This course is designed for the System Administrator role and aligns with the NICE requirements for system administration on specialized cyber defense applications and systems (e.g, antivirus, audit, and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.

DES 216 – Protecting Cloud Infrastructure (UPDATED) (40 mins)

This course provides DevOps Engineers, IT Architects and Network Engineers responsible for the security of applications and data with the skills and knowledge required to protect their organization's cloud infrastructure.

Topics Include:

- The role of Data Encryption
- Identity and Authentication
- Firewalls and Network Security (SDNs, VPNs, DMZs)
- Division of Duties
- Compliance requirements
- Securing VM and Containers

DES 218 – Protecting Microservices, Containers, and Orchestration (UPDATED) (30 mins)

Using Microservices, organizations can isolate software functionality into multiple independent modules that are individually responsible for performing precisely defined, standalone tasks communicating with each other through simple, universally accessible application programming interfaces (APIs). Containers enable developers to simultaneously build and ship these microservices; integrate them with other systems and automatically orchestrate them using predefined rules and processes.

This course is designed to educate DevOps Engineers, IT Architects, and Network Engineers working in Linux or on the cloud to add value to the application lifecycle through proper orchestration and enable faster development and fault-prone provisioning and configurations.

Topics Include:

- Hardening the OS
- Vulnerability Scanning
- Docker, SELinux and AWS Microservices
- API Gateways

- Node monitoring with Prometheus
- Implementing OAuth
- Schedulers and Orchestrators
- Defining a Pod Security Policy
- Using Metadata Concealment

DSO 303 – Automating Security Updates (20 mins)

Essential to keeping systems secure, reducing risk, introducing new or enhanced features, or improving compatibility, software updating can be challenging and resource-intensive. Automating this process eliminates routine tasks and frees up administrative time. This course introduces automation procedures for systems administration to effectively and efficiently manage IT software in adherence to functional and security requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Employ automated mechanisms to implement changes to the current system baseline and deploy the updated baseline across the installed base
- Review system changes to determine whether unauthorized changes have occurred
- Remove previous versions of software or firmware components after installing updated versions
- Ensure that security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures

---

DSO 305 – Automating CI/CD Pipeline Compliance (20 mins)

The adoption of cloud infrastructure and DevOps requires consistent integration of security to achieve a reliable lifecycle of continuous deployment. Integrating compliance into the CI/CD Pipeline requires a coordinated effort by everyone involved in the development pipeline. This course enables learners to automate the implementation of security tasks across the CI/CD pipeline in adherence to compliance requirements.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Automate scanning and reporting tasks to ensure privacy policies, applicable laws, regulations, and service-level agreements are reviewed and documented for compliance regulations
- Identify and document controls owned by outside parties
- Configure change monitors to identify changes to organizational systems and environments of operation that may affect security and privacy risk
- Verify that all control objectives are met, and all key controls are designed and operating effectively

---

ENG 110 – Essential Account Management Security (15 mins)

This infrastructure security course provides essential guidance on implementing specific account management security controls at the hardware and software level to facilitate compliance with applicable regulatory requirements.

Topics include:

- How to define and control network access
- Creating a separation of duties policy
- Building and managing segregation of resources strategies
- Monitoring system access
- Using digital certificates for authentication

ENG 111 – Essential Session Management Security (15 mins)

This infrastructure security course provides guidance to system designers and developers on how to implement session management controls at the software level. These techniques enhance security of web applications and facilitates compliance with applicable regulatory requirements.

Topics include:

- Securing session identifiers

- Implementing Transport Layer Security (TLS) so sensitive data is always transmitted over secure channels
- Ensuring client browsers send cookies over HTTPS connections

---

ENG 112 – Essential Access Control for Mobile Devices (15 mins)

This infrastructure security course teaches designers and developers how to implement software-level access controls on mobile devices to mitigate threats, protect privacy, and comply with applicable regulatory requirements.

Topics include:

- Identifying threats to mobile devices
- The importance of protecting user privacy and confidentiality
- Methods for encrypting data at rest and data in transit
- Implementing application code signing to ensure software integrity

---

ENG 113 – Essential Secure Configuration Management (15 mins)

This infrastructure security course trains program managers, system designers, and developers on proper security practices for defining and implementing IT system configuration management.

Topics include:

- Key configuration practices and configuration change control
- Security impact analysis
- Access restrictions for change
- Principle of least functionality
- Information system component inventory

ENG 119 – Essential Security Audit & Accountability (15 mins)

This infrastructure security course trains information system owners, system administrators, and information system security officers on how to build and communicate effective audit policies and controls.

Topics include:

- Documenting security audits
- Implementing audit controls
- Using audit tools
- Generating audit reports

ENG 121 – Essential Identification & Authentication (15 mins)

This infrastructure security course teaches those responsible for information security how to develop identification and authentication policy and controls. The course spans personnel, devices, and information systems.

Topics include:

- Identification and authentication of users inside and outside your organization
- Device identification and authentication
- Identifier management
- Authenticator management and feedback
- Cryptographic module authentication
- Service identification and authentication
- Adaptive identification and authentication
- Processes for re-authentication

ENG 122 – Essential Physical & Environmental Protection (15 mins)

This infrastructure security course educates those responsible for developing physical and environmental protection policies how to create effective controls and comply with applicable regulatory requirements.

Topics include:

- Physical access authorizations and control
- Access control for transmission medium and output devices
- Monitoring physical access
- Information leakage, asset monitoring and tracking

ENG 125 – Essential Data Protection (15 mins)

This infrastructure security course delivers training to personnel in information systems, information security, systems design, software development, and IT operations on essential data security techniques. Focus is primarily on cryptographic controls at the information systems level and compliance with applicable regulatory requirements.

Topics include:

- Asymmetric key algorithms
- Using hash functions to protect data integrity
- Proper password storage for authentication purposes
- Encrypting file transfers and downloads
- Adding salt values before hashing
- Using Certificate Authorities

ENG 127 – Essential Media Protection (15 mins)

This infrastructure security course describes the development and dissemination of an organization-wide information media protection policy that addresses scope, roles, responsibilities, and coordination among organizational entities to facilitate compliance with applicable regulatory requirements.

Topics include:

- Best practices for media protection
- Controls for marking, storage, and transport of media
- Media sanitization and downgrading

Systems Architecture (ARC)

COD 160 -Fundamentals of Secure Embedded Software Development (45 mins)

Embedded devices tend to be linked to other devices via a wide array of technologies and often susceptible to targeted attacks. This course identifies security issues inherent to embedded devices and their deployment environments. You will also learn about the appropriate constraint of functionality from a security standpoint, and techniques to prevent common vulnerabilities.

Topics include:

- Techniques to identify system security and performance requirements
- Developing appropriate security architecture
- Selecting the correct mitigations
- How to develop policies that can ensure the secure operation of your system

---

COD 201 – Secure C Encrypted Network Communications (15 mins)

This course explores secure communications using Transport Layer Security (TLS) and best practices for implementing these within C and C++ applications.

Topics include:

- Key principles of TLS
- Libraries and interfaces for implementing the TLS protocol
- TLS security considerations
- Alternatives to TLS

COD 216 – Leveraging .NET Framework Code Access Security (CAS) (30 mins)

This course explores the foundation of .NET, the CLR's native security infrastructure (Code Access Security), and the ASP.NET security infrastructure.

Topics include:

- Differences between managed and unmanaged code
- Access control functions in Windows
- Code Access Security (CAS) functions in .NET
- Interactions between Windows access control and CAS
- Key aspects of ASP.NET security and understand the Level 2 Security Transparency Model

---

COD 217 – Mitigating .NET Security Threats (45 mins)

With a primary focus on .NET secure error handling and secure logging, this course describes secure coding techniques to avoid information disclosure and other vulnerabilities.

Topics include:

- Avoiding dangerous patterns when using CAS
- Avoiding common .NET security pitfalls
- Ensuring application fail safely

COD 241 – Creating Secure Oracle DB Applications (45 mins)

This secure coding course introduces database application developers to key industry best practices for data security.

Topics include:

- Secure query construction
- Secure communication and storage
- Creating safe stored procedures to prevent SQL Injection
- How to secure data at rest and data in transit using Oracle Database features

---

COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)

This secure coding course explores protecting sensitive data and ensuring the integrity of applications running on the Microsoft SQL Server Engine and Azure SQL Database.

Topics include:

- The security function of roles in controlling user and principal access to SQL Server securables
- Exercising fine-grained controls that adhere to the Principle of Least Privilege
- Leveraging the security features of Microsoft's Azure SQL Database to protect sensitive data and ensure the integrity of your applications

---

COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Ruby on Rails. After completing this course, you will be able to identify and mitigate injection vulnerabilities, such as SQL injection and cross-site scripting, build strong session management into your Rails applications, and prevent other common vulnerabilities, such as cross-site request forgery and direct object access.

Topics include:

- How to identify and mitigate injection vulnerabilities: SQL Injection (SQLi) and cross-site scripting (XSS)
- How to build strong session management into your rails applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF) and direct object access

---

COD 257 – Creating Secure Python Web Applications (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Python. After completing this course, you will be able to understand various types of injection vulnerabilities, including SQL injection and cross-site scripting. You will also be able to understand how to build strong session management into your Python web applications and how to prevent common vulnerabilities, such as cross-site request forgery, direct object access, and others.

Finally, you will be able to recognize file system threats to web applications, including vulnerabilities with path traversal, temporary files, and insecure client redirects.

Topics include:

- Types of Injection Vulnerabilities including SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- File system threats to web applications including vulnerabilities with path traversal, temporary files, and insecure client redirects
- How to build strong session management into your python web applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF), direct object access, and others

---

COD 258 – Creating Secure PHP Web Applications (30 mins)

In this course, you will learn important concepts for secure PHP scripting. After completing this course, you will be able to use quotation marks correctly, discuss techniques for handling return codes and exceptions, canonicalize paths to identify the correct files, identify dangerous functions to avoid, apply techniques for preventing or mitigating different injection vulnerabilities, recognize that regular expressions must be handled carefully to avoid DoS attacks, and describe techniques to protect sensitive data in transit.

Topics covered:

- Key defensive coding principles such as proper session management, error handling, authentication, authorization, data storage, and use of encryption
- Avoiding and mitigating vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), File Inclusion, Command Injection, Cross-Site Request Forgery (CSRF) and Null Byte attacks

---

COD 270 – Creating Secure COBOL & Mainframe Applications (25 mins)

This secure coding course covers countermeasures for security vulnerabilities on mainframe systems such as input validation, parameterized APIs, strong cryptography, and memory management issues.

Topics include:

- Identifying vulnerabilities and threats to mainframe applications and data
- Mitigating SQL injection threats using safe prepared statements and parameterized APIs
- Validating all input
- Using exec* functions instead of system functions to mitigate the risk of command injection
- Using key derivation functions to protect stored password
- Encrypting sensitive data at rest using AES-256
- Protecting sensitive data in transit with TLS
- Preventing deadlocks by using the ENQ and DEQ commands
- Avoiding manual memory management in order to prevent buffer overflow conditions

---

COD 281 – Java Security Model (20 mins)

In this secure coding course, you will learn about Java's policy-driven security model and how to leverage it to build more secure applications.

Topics include:

- Java security model components
- Functions of the Java security manager and access controller
- Java security policies and the Java security policy files

COD 283 – Java Cryptography (45 mins)

This secure coding course explores the key concepts of public key cryptography and teaches you how to use the Java keytool command-line utility for creating and managing keys and keystores.

Topics include:

- How public and private key pairs work together to encrypt and decrypt data for secure transfer and to create and verify digital signature
- Generating secure encryption keys and identifying related issues such as pseudo random number generators (PRNGs), key derivation functions, and initialization vectors
- Selecting an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode

---

COD 285 – Developing Secure Angular Applications (30 mins)

Widely adopted amongst the software development community because of the versatility it provides, securing angular applications comes with a steep learning curve. While component-based architecture is one of the key benefits of using angular, managing components can be complicated. This course is designed to develop the skills required to design, build, and maintain secure Angular applications following software assurance best practices.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure Angular.js compliance requirements, including:

- Securing AngularJS templates to help mitigate threats from expression Injection and dynamically loading templates from untrusted sources
- Ensuring that both the server and the client cooperate to eliminate these threats and potential security issues that need to be blocked
- Implementing Content Security Policies and secure routing

COD 286 – Creating Secure React User Interfaces (10 mins)

This JavaScript library has become a popular choice in the market because of its ability to help solve web development challenges. The framework makes it painless to create interactive user interfaces, design simple view, and reactively update to changes. This course is designed to develop the skills required to securely build user interfaces using multiple components and implement best practices to avoid common attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure React.js User Interfaces compliance requirements, including:

- Creating secure React components
- Avoiding vulnerable third-party React component libraries
- Preventing React component injection attacks
- Using and serializing JSON

COD 363- Securing HTML5 Data (20 mins)

In this course, you will learn about new features that raise security issues in HTML5 forms, security issues surrounding local data storage, best practices for HTML5 connectivity with the WebSocket API and Server-ent Events, and best practices for the Web Workers, History, Geolocation, and Drag and Drop APIs.

COD 382 – Protecting Data in Java (30 mins)

This course discusses protecting data at rest and in transit in Java applications. Several code examples are provided to illustrate key concepts.

After completing this course, you will be able to protect data at rest appropriate cryptographic techniques and protect data in transit with appropriate cryptographic techniques.

COD 383 – Protecting Java Backend Services (30 mins)

Backends are designed for applications that need faster performance, large amounts of addressable memory, and continuous or long-running background processes. The versatility of Java enables developers to design and deliver the right business solutions however their efficiency requires distinctive experiencer and great expertise.

This course aims to provide software developers and DevOps Engineers with the next level understanding of best practices for developing back end frameworks using Java while developing skills necessary to handle user input and build secure systems.

Topics Include:

- The Function of OAuth2 and JWT
- How to leverage the JAAS API
- The advantages of the Spring Security framework
- Validating Length Before Applying RegEx
- Protecting Sensitive Data in Transit Using TLS
- How to identify and protect against SQLi, HQLi, XXE, CSRF, and RegEx DoS attacks

---

DES 101 – Fundamentals of Secure Architecture (20 mins)

In the past, software applications were created with little thought to the importance of security. Recently, businesses have become more rigorous about how they buy and deploy software as security is a large part of the total cost that risk software applications inherently carry. In this course, you examine the state of the industry from a security perspective, setting the foundation for secure software development.

Topics include:

- Application security architecture principles
- Lessons learned: security disasters in software design
- How to use confidentiality, integrity, and availability to drive better security design decisions

---

DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)

This course introduces three important elements of cryptographic systems: random number generation, algorithms and keys.

Topics include:

- The critical role of randomness in cryptography
- Common algorithms to perform cryptographic manipulation of information
- Types and roles of cryptographic keys
- The key management problem
- Common types of digital certificates and its creation process
- Components and roles of a public key infrastructure
- Weaknesses in the digital certificate trust mode
- Mechanisms to manage and distribute cryptographic keys

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 204 – Role of Cryptography in Application Development (15 mins)

This course introduces cryptography and how cryptography can help secure software applications and data. It also provides an overview of common uses of cryptography.

Topics include:

- Identifying relevant cryptographic technologies
- Knowing common “data-in-motion” crypto options and the strengths/weaknesses of each
- Applying common “data-at-rest” crypto options and the strengths/weaknesses of each

---

DES 205 – Message Integrity Cryptographic Functions (45 mins)

This course explains how encrypting and signing a message works, how message authentication codes work, and why a digital signature is superior to a cryptographic hash for validating software integrity.

Topics include:

- Message integrity function is its value
- The difference between a message authentication code and a digital signature
- How a digital signature works
- Encrypting and signing messages
- Message authentication codes
- Digital signature vs. a cryptographic hash for validating software integrity

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 212 – Architecture Risk Analysis & Remediation (30 mins)

This course defines concepts, methods, and techniques for analyzing the architecture and design of a software system for security flaws. Special attention is given to analysis of security issues in existing applications; however, the principles and techniques are applicable to systems under development. Techniques include accurately capturing application architecture, threat modeling with attack trees, attack pattern analysis, and enumeration of trust boundaries.

Topics include:

- How to assess design components for security flaws
- The use and value of threat modeling and attack surface analysis
- Techniques to remove architecture weak spots and avoid vulnerability propagation

---

DES 255 – Securing the IoT Update Process (30 mins)

Addressing updates across the Internet of Things (IoT) can be complicated due to the complex ecosystems of connected devices deployed across multiple environments. This course aims to educate learners to establish a secure, scalable update process for IoT devices.

After completing this course, you will be able to:

- Identify the risks of delivering IoT device updates
- Understand each phase in the IoT update process
- Determine considerations for the secure delivery of updates to the vehicle
- Securely design, develop, delivery, and install IoT update

DES 260 – Fundamentals of IoT Architecture & Design (30 mins)

This course focuses on topics related to architecting and designing a secure Internet of Things (IoT) system. Particular emphasis is placed on embedded IoT devices and their relationship with cloud services.

After completing this course, you will have a deep understanding of an IoT system, its components, and the security implications of various design choices.

Topics include:

- Elements to be reviewed and defined in the requirements phase
- Authorization considerations within the IoT device itself as well as connected components
- Designing a secure IoT architecture
- Authentication to validate the identity of users and devices
- Logical access controls to ensure users are granted appropriate levels of service
- Physical security concerns to protect access to IoT devices
- Monitor communications throughout the IoT system
- Secure communications between the various system components

---

DES 306 – Creating a Secure Blockchain Network (20 mins)

While Blockchain technology continues to emerge for its ability to improve data security, speed up transactions and save costs, it comes with its advantages it comes with a wide array of challenges. Properly securing a blockchain network begins with the implementation of strong authentication and cryptography key vaulting mechanisms. This course provides learners with an understanding of the essential requirements for creating a secure blockchain network.

After completing this course you will be able to:

- Identify operational, legal and compliance requirements
- Create a blockchain threat model
- Create blockchain trust policies, access controls, and smart contracts
- Manage identity, access, entitlements, certificates, and keys
- Monitor, report, and manage incidents

DES 311 – Creating Secure Application Architecture (45 mins)

Architecting secure solutions is paramount to ensure developers do not incorporate insecure components, which could introduce hundreds of individual security vulnerabilities in the as-built system. This course covers a set of key security principles to improve the security of application architecture and design.

Topics include:

- Applying defense to harden applications and make them more difficult for intruders to breach
- Reducing the amount of damage an attacker can accomplish
- Compartmentalizing to reduce the impact of exploits
- Using centralized input and data validation to protect applications from malicious input
- Reducing the risk in error code paths

DES 312 – Protecting Cardholder Data (20 mins)

While cardholder data consists of any personally identifiable information (PII) associated with a person who has a credit or debit card, the PCI Secure Standards Council (PCI SSC) has specific requirements to protect cardholder data at all times. Despite common misconceptions, this also includes account numbers, expiration date, and/or service code as cardholder data. This course is designed to provide Information Systems Security Developers with the knowledge needed to minimize the storage of cardholder data and take necessary precautions to protect it in adherence to the PCI Software Security Framework and NIST 800-53 Guidelines.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Ensuring the software does not store sensitive authentication data after authorization, even if encrypted unless the software is intended only for use by issuers or organizations that support issuing services.
- Rendering the Primary Account Number (PAN) is unreadable anywhere it is stored.
- Guiding customers regarding the secure deletion of cardholder data after the expiration of the customer-defined retention period.

DSO 302- Automated Security Testing (20 mins)

Modern application development, increasing speed-to-market requirements, and assuring application security have made automated security testing a top priority for many organizations. Automating Security Testing can be difficult and daunting, but incorporating into workflows can provide consistency, expedience, and ensure software quality. This course teaches learners to integrate the built-in strengths of DevOps within the security Testing process while adhering to security testing needs.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Understanding the importance of orchestrating secure system and service configuration
- Determining which types of automated tests should be performed at various stages of the software development lifecycle
- Creating policies that support simultaneous testing and building in keeping with DevSecOps secure software development
- Leveraging Information Security Continuous Monitoring (ISCM) tools to perform a broad range of tasks, including periodic security and vulnerability scans of all system components

---

DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)

APIs are a critical component of cloud computing, and modern development fueling the success of DevOps. This course enables learners to implement mechanisms to securely manage API requests through the use of API gateways in DevOps and serverless environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Deployment of secure API gateways through the implementation of core features such as to request and response collapsing API Transformation, and Protocol Translation for microservice-based applications
- Implement secure Identity and Access Management (IAM) across all services
- Provide certificate management, secrets management, and encryption services
- Leverage APIs to gather, synthesize and alert on security-relevant events as part of a comprehensive cybersecurity risk management program

---

Systems Development (SYS)

COD 241 – Creating Secure Oracle DB Applications (45 mins)

This secure coding course introduces database application developers to key industry best practices for data security.

Topics include:

- Secure query construction
- Secure communication and storage
- Creating safe stored procedures to prevent SQL Injection
- How to secure data at rest and data in transit using Oracle Database features

---

COD 242 – Creating Secure SQL Server & Azure SQL DB Applications (40 mins)

This secure coding course explores protecting sensitive data and ensuring the integrity of applications running on the Microsoft SQL Server Engine and Azure SQL Database.

Topics include:

- The security function of roles in controlling user and principal access to SQL Server securables
- Exercising fine-grained controls that adhere to the Principle of Least Privilege
- Leveraging the security features of Microsoft's Azure SQL Database to protect sensitive data and ensure the integrity of your applications

---

COD 246 – PCI DSS 3: Protecting Stored Cardholder Data (15 mins)

In this course, you will learn how to use the CWE-311 guidelines to identify, test and mitigate for missing encryption of sensitive data. Coverage includes techniques for spotting missing encryption through code review and testing. Secure coding best practices are included, as well as descriptions of technology-specific weaknesses as appropriate. This course requires basic knowledge of client-server applications, web applications, the Software Development Life Cycle, cryptography, and the STRIDE model.

COD 247 – PCI DSS 4: Encrypting Transmission of Cardholder Data (15 mins)

In this course, you will learn about the risks of insecure communications and how to use the CWE guidelines, specifically the OWASP Top Ten, to mitigate these risks. Coverage includes techniques for spotting missing encryption and using Transport Layer Security (TLS).

COD 248 – PCI DSS 6: Develop and Maintain Secure Systems and Applications (15 mins)

In this course, you will learn to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities. Coverage will be aligned with the CWE SANS Top 25 and OWASP 2017 Top 10 vulnerability frameworks.

COD 251 – Defending AJAX-Enabled Web Applications (25 mins)

This course introduces fundamentals of how to defend AJAX-enabled Web applications, including the difference between regular and AJAX-enabled web applications, AJAX security checks against challenges, and common attacks against AJAX-enabled applications.

Topics include:

- Architectural differences between regular web applications and AJAX-enabled applications
- Identifying threats to AJAX applications: cross-site scripting (XSS), cross-site request forgery (CSRF), and injection attacks
- Implementing countermeasures against attacks: protecting client resources, validating input, protecting web services requests, preventing request forgeries, and securing data access.

COD 253 – Creating Secure AWS Cloud Applications (45 mins)

This course examines the security vulnerabilities, threats, and mitigations for AWS cloud computing services and provides best practices for securing Web applications by leveraging AWS platform security features.

Topics include:

- AWS security features: Key Management Service (KMS), Hardware Security Module (HSM), Identity and Access Management (IAM), and CloudWatch
- How to leverage security features built into Common Amazon Cloud services such as Simple Storage Service (S3), Elastic Compute Cloud (Amazon EC2), Elastic Block Store (EBS), Amazon Glacier, Relational Database Service (RDS), DynamoDB, Elastic MapReduce (EMR), and Amazon Machine Images (AMI)

COD 254 – Creating Secure Azure Applications (45 mins)

This course examines key Azure security platforms and services that you can use to improve the security of your applications.

Topics include:

- Security vulnerabilities, threats, and mitigations for Azure cloud computing services
- How to identify common security threats to cloud-based applications
- Secure coding best practices to mitigate threats
- How to leverage built-in Azure features for an extra layer of defense

---

COD 255 – Creating Secure Code: Web API Foundations (20 mins)

This secure coding course introduces the fundamentals of secure web services development.

Topics include:

- Common web services threats that put your application at risk
- Impact of web services attacks
- Secure development best practices to protect web services

COD 256 – Creating Secure Code: Ruby on Rails Foundations (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Ruby on Rails. After completing this course, you will be able to identify and mitigate injection vulnerabilities, such as SQL injection and cross-site scripting, build strong session management into your Rails applications, and prevent other common vulnerabilities, such as cross-site request forgery and direct object access.

Topics include:

- How to identify and mitigate injection vulnerabilities: SQL Injection (SQLi) and cross-site scripting (XSS)
- How to build strong session management into your rails applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF) and direct object access

---

COD 257 – Creating Secure Python Web Applications (45 mins)

In this course, you will learn about best practices and techniques for secure application development with Python. After completing this course, you will be able to understand various types of injection vulnerabilities, including SQL injection and cross-site scripting. You will also be able to understand how to build strong session management into your Python web applications and how to prevent common vulnerabilities, such as cross-site request forgery, direct object access, and others.

Finally, you will be able to recognize file system threats to web applications, including vulnerabilities with path traversal, temporary files, and insecure client redirects.

Topics include:

- Types of Injection Vulnerabilities including SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- File system threats to web applications including vulnerabilities with path traversal, temporary files, and insecure client redirects
- How to build strong session management into your python web applications
- Preventing common vulnerabilities such as cross-site request forgery (CSRF), direct object access, and others

---

COD 258 – Creating Secure PHP Web Applications (30 mins)

In this course, you will learn important concepts for secure PHP scripting. After completing this course, you will be able to use quotation marks correctly, discuss techniques for handling return codes and exceptions, canonicalize paths to identify the correct files, identify dangerous functions to avoid, apply techniques for preventing or mitigating different injection vulnerabilities, recognize that regular expressions must be handled carefully to avoid DoS attacks, and describe techniques to protect sensitive data in transit.

Topics covered:

- Key defensive coding principles such as proper session management, error handling, authentication, authorization, data storage, and use of encryption
- Avoiding and mitigating vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), File Inclusion, Command Injection, Cross-Site Request Forgery (CSRF) and Null Byte attacks

---

COD 259 – Node.js Threats & Vulnerabilities (30 mins)

In this secure coding course, you will learn about system configuration, injection attacks, session management, package management, and the AngularJS framework, all within the context of Node.js security.

Topics include:

- Best practices for Node.js server and system configuration
- Types of injection attacks and mitigation techniques
- Proper settings for session cookie security
- Mitigating cross-site request forgery (CSRF) attacks
- Leveraging popular static analysis tools for Node.js
- Understand why templates and expressions are vulnerable to injection
- Methods, services, elements, and parameters that should not be used with untrusted data
- Best practices for loading templates

COD 261 – Threats to Scripts (30 mins)

In this secure coding course, you will learn about the impact of incorrect script development or lax security measures.

Topics include:

- Outcomes of vulnerable scripts
- Common scripting vulnerabilities such as SQL Injection (SQLi)
- Security issues related to permissions and privileges
- Impact of different types of resource

COD 262 – Fundamentals of Shell and Interpreted Language Security (30 mins)

In this secure coding course, you will learn about how shell scripting languages compare with more modern interpreted languages with respect to security features, and defensive coding techniques, and dealing with common differences between platforms that can alter script behavior.

Topics incude:

- Information security principles including least privilege and defense in depth
- The importance of data validation and how to validate using input, array indices, and environment variables
- Using file system operations safely to protect
- Preventing or mitigating cached secret disclosure
- The importance of up-to-date communication security techniques
- Operating system (OS) system portability issues

COD 263 – Secure Bash Scripting (15 mins)

In this secure coding course, you will learn about the importance of error and exception handling in shell scripts and interpreted languages such as Perl, Python, Bash and Ruby.

Topics covered:

- Techniques for handling errors and exceptions in shell scripts and interpreted languages
- Common syntax pitfalls and dangerous functions to avoid
- Techniques for preventing/mitigating different vulnerabilities including different types of injection

---

COD 264 – Secure Perl Scripting (15 mins)

Perceived as being difficult to fix in comparison to other programming languages Perl is commonly known as “the duct-tape of the Internet.” This general-purpose programming language is currently being used for a wide range of tasks as it takes the best features from other languages.

In this course, you will learn about best practices for secure scripting in Perl, features of Perl’s taint mode, handling errors in Perl, protecting files, preventing format string and injection vulnerabilities, using regular expressions carefully, and protecting sensitive data in transit with Transport Layer Security (TLS).

COD 265 – Secure Python Scripting (15 mins)

In this secure coding course, you will learn important concepts for secure Python scripting including techniques for error and exception handling.

Topics Covered:

- Avoiding uncontrolled format string vulnerabilities
- Defending against Regular Expression Denial of Service (DoS) attacks
- Protecting sensitive data in transit
- Techniques for preventing/mitigating different vulnerabilities including different types of injection

---

COD 266 – Secure Ruby Scripting (15 mins)

In this secure coding course, you will learn important concepts for secure Ruby scripting, techniques for preventing/mitigating different vulnerabilities including different types of injection, and protecting sensitive data in transit.

Topics covered:

- Validating command-line parameters
- Using quotation marks correctly
- Using unmask to set default file permissions
- Protecting files and canonicalizing paths
- Defending against Regular Expression Denial of Service (DoS) attacks

---

COD 267 – Securing Python Microservices (30 mins)

Microservices have become widely popular, replacing complicated XML-based schemas and service-oriented architectures (SOA) because of the ability to create separate, well-defined, individual components within a system. By leveraging python microservices, complex applications can be broken down into these components to ease further development and deployment.

This course will provide cloud developers, python developers, and software architects with a working knowledge of possible attacks, how to secure interaction between services and an understanding of how to implement basic principles to ensure the security of python microservices.

Topics Include:

- Techniques for handling return codes and exceptions
- Canonicalizing paths to identify the correct files
- Identifying dangerous functions
- Applying techniques for mitigating injection vulnerabilities
- How to securely handle regular expressions
- How to protect sensitive data

COD 281 – Java Security Model (20 mins)

In this secure coding course, you will learn about Java's policy-driven security model and how to leverage it to build more secure applications.

Topics include:

- Java security model components
- Functions of the Java security manager and access controller
- Java security policies and the Java security policy files

COD 283 – Java Cryptography (45 mins)

This secure coding course explores the key concepts of public key cryptography and teaches you how to use the Java keytool command-line utility for creating and managing keys and keystores.

Topics include:

- How public and private key pairs work together to encrypt and decrypt data for secure transfer and to create and verify digital signature
- Generating secure encryption keys and identifying related issues such as pseudo random number generators (PRNGs), key derivation functions, and initialization vectors
- Selecting an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode

---

COD 284 – Secure Java Coding (30 mins)

In this course, you will learn about secure Java coding practices, including techniques for avoiding Denial of Service (DoS) and regular expression DoS attacks, and guidelines for secure error handling and logging. You will also become familiar with the dangers of unreleased resources, null references, and XML external entity (XXE) attacks

Topics include:

- Denial of Service and designing your application to handle or avoid such situations
- Guidelines for secure error handling and logging
- Identify the dangers of unreleased resources, null references, and XML external entity attacks

---

COD 285 – Developing Secure Angular Applications (30 mins)

Widely adopted amongst the software development community because of the versatility it provides, securing angular applications comes with a steep learning curve. While component-based architecture is one of the key benefits of using angular, managing components can be complicated. This course is designed to develop the skills required to design, build, and maintain secure Angular applications following software assurance best practices.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure Angular.js compliance requirements, including:

- Securing AngularJS templates to help mitigate threats from expression Injection and dynamically loading templates from untrusted sources
- Ensuring that both the server and the client cooperate to eliminate these threats and potential security issues that need to be blocked
- Implementing Content Security Policies and secure routing

COD 286 – Creating Secure React User Interfaces (10 mins)

This JavaScript library has become a popular choice in the market because of its ability to help solve web development challenges. The framework makes it painless to create interactive user interfaces, design simple view, and reactively update to changes. This course is designed to develop the skills required to securely build user interfaces using multiple components and implement best practices to avoid common attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet Secure React.js User Interfaces compliance requirements, including:

- Creating secure React components
- Avoiding vulnerable third-party React component libraries
- Preventing React component injection attacks
- Using and serializing JSON

DES 202 – Cryptographic Suite Services: Encoding, Encrypting & Hashing (45 mins)

This course presents an overview of the fundamental services provided by cryptographic suites, namely encoding, encrypting, and hashing.

Topics include:

- Encoding and decoding
- Encryption and decryption
- The difference between encoding and encryption
- The value and application of hashing
- Where, when, and how to use crypto

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s): K0018: Knowledge of encryption algorithms.

DES 203 – Cryptographic Components: Randomness, Algorithms, and Key Management (15 mins)

This course introduces three important elements of cryptographic systems: random number generation, algorithms and keys.

Topics include:

- The critical role of randomness in cryptography
- Common algorithms to perform cryptographic manipulation of information
- Types and roles of cryptographic keys
- The key management problem
- Common types of digital certificates and its creation process
- Components and roles of a public key infrastructure
- Weaknesses in the digital certificate trust mode
- Mechanisms to manage and distribute cryptographic keys

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 204 – Role of Cryptography in Application Development (15 mins)

This course introduces cryptography and how cryptography can help secure software applications and data. It also provides an overview of common uses of cryptography.

Topics include:

- Identifying relevant cryptographic technologies
- Knowing common “data-in-motion” crypto options and the strengths/weaknesses of each
- Applying common “data-at-rest” crypto options and the strengths/weaknesses of each

---

DES 205 – Message Integrity Cryptographic Functions (45 mins)

This course explains how encrypting and signing a message works, how message authentication codes work, and why a digital signature is superior to a cryptographic hash for validating software integrity.

Topics include:

- Message integrity function is its value
- The difference between a message authentication code and a digital signature
- How a digital signature works
- Encrypting and signing messages
- Message authentication codes
- Digital signature vs. a cryptographic hash for validating software integrity

This course aligns with the National Initiative for Cybersecurity Education (NICE) requirement(s):

- K0018: Knowledge of encryption algorithms
- K0019: Knowledge of cryptography and cryptographic key management concepts

---

DES 255 – Securing the IoT Update Process (30 mins)

Addressing updates across the Internet of Things (IoT) can be complicated due to the complex ecosystems of connected devices deployed across multiple environments. This course aims to educate learners to establish a secure, scalable update process for IoT devices.

After completing this course, you will be able to:

- Identify the risks of delivering IoT device updates
- Understand each phase in the IoT update process
- Determine considerations for the secure delivery of updates to the vehicle
- Securely design, develop, delivery, and install IoT update

DES 311 – Creating Secure Application Architecture (45 mins)

Architecting secure solutions is paramount to ensure developers do not incorporate insecure components, which could introduce hundreds of individual security vulnerabilities in the as-built system. This course covers a set of key security principles to improve the security of application architecture and design.

Topics include:

- Applying defense to harden applications and make them more difficult for intruders to breach
- Reducing the amount of damage an attacker can accomplish
- Compartmentalizing to reduce the impact of exploits
- Using centralized input and data validation to protect applications from malicious input
- Reducing the risk in error code paths

DES 312 – Protecting Cardholder Data (20 mins)

While cardholder data consists of any personally identifiable information (PII) associated with a person who has a credit or debit card, the PCI Secure Standards Council (PCI SSC) has specific requirements to protect cardholder data at all times. Despite common misconceptions, this also includes account numbers, expiration date, and/or service code as cardholder data. This course is designed to provide Information Systems Security Developers with the knowledge needed to minimize the storage of cardholder data and take necessary precautions to protect it in adherence to the PCI Software Security Framework and NIST 800-53 Guidelines.

Upon successful completion of this course, learners will have the knowledge and skills required to meet privacy compliance requirements, including:

- Ensuring the software does not store sensitive authentication data after authorization, even if encrypted unless the software is intended only for use by issuers or organizations that support issuing services.
- Rendering the Primary Account Number (PAN) is unreadable anywhere it is stored.
- Guiding customers regarding the secure deletion of cardholder data after the expiration of the customer-defined retention period.

DSO 253 – DevSecOps in the AWS Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure AWS services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Implement inventory and configuration controls and services, including AWS Config, AWS CloudFormation, and Amazon Inspector
- Ensure Infrastructure Security using Amazon VPC, AWS WAF, Customer-controlled encryption and automatic encryption of all traffic
- Mitigate DDoS threats with Autoscaling, Amazon CloudFront and Amazon Route 53
- Encrypt data using AWS Key Management Services (KMS), Server-side encryption (SSE), AWS CloudHSM; and leverage EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift encryption features
- Meet Monitoring and Logging requirements using AWS CloudTrail and Amazon CloudWatch
- Use Identity and Access Controls to define, enforce, and manage user access policies with AWS Identity and Access Management (IAM), AWS Multi-Factor Authentication and AWS Directory Services
- Understand AWS policies for customer Penetration Testing

DSO 254 – DevSecOps in the Azure Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. Provides learners with an understanding of how to align and configure Azure services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Identify and manage the data, personnel, devices, systems, and facilities to meet the organization's business objectives and risk strategy
- Protect assets and associated facilities by using Access Control, limiting access to authorized users, processes, or devices, and to authorized activities and transactions
- Protect data-at-rest and data-in-transit by leveraging security services such as Azure Storage Service Encryption, Azure Backup Data Encryption, Azure SQL Transparent Data Encryption BitLocker, Azure VPN Gateway
- Detect anomalous activity in a timely manner and understand the potential impact of events by using Azure Security Center, Advanced Threat Analytics, Design and Implementation for Active Directory (DIAD), SIEM integration and Cloud App Security
- Ensure response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events

---

DSO 304 – Securing API Gateways in a DevSecOps Framework (20 mins)

APIs are a critical component of cloud computing, and modern development fueling the success of DevOps. This course enables learners to implement mechanisms to securely manage API requests through the use of API gateways in DevOps and serverless environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Deployment of secure API gateways through the implementation of core features such as to request and response collapsing API Transformation, and Protocol Translation for microservice-based applications
- Implement secure Identity and Access Management (IAM) across all services
- Provide certificate management, secrets management, and encryption services
- Leverage APIs to gather, synthesize and alert on security-relevant events as part of a comprehensive cybersecurity risk management program

DSO 306 – Implementing Infrastructure as Code (20 mins)

Used to automate infrastructure deployment processes, Implementing Infrastructure as Code comes with a unique set of challenges making it hard for organizations to maintain agility, control, and visibility. This course is designed to help developers leverage Infrastructure as Code to securely and effectively launch cloud environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Using tools in the development stage to help convert requirements into source code
- Leveraging the security features available in most integrated development environments (IDEs) for multiple programming language support
- Identify and mitigate the most common IaC vulnerabilities, including Weak Authentication Tokens, Disclosure of Authentication Credentials, Excessive Privileges or Capabilities, Misconfigured Network Filtering, and Missing Encryption

---

DSO 307 – Secure Secrets Management (20 mins)

As the need to protect critical data increases, organizations must focus efforts on improving processes used to manage essential information. This course is designed to ensure software development teams employ appropriate techniques to manage identities, privileges, and secrets securely.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Ensuring that approved cryptographic algorithms and methods are used for securing critical assets
- Aligning key-management processes and procedures with those recognized by industry-standards bodies
- Using Approved Random Number Generators| Providing strong entropy when Using Random Number Generator

---

ENG 115 – Essential System & Information Integrity (15 mins)

This infrastructure security course provides essential guidance to program managers, system designers and developers on how to identify systems affected by software flaws, assess potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel.

Topics include:

- Flaw remediation
- Malicious code protection
- Information system monitoring
- Software, firmware, and information integrity
- Information input validation
- Error handling
- Information handling and retention
- Information output filtering
- Memory protection

ENG 116 – Essential Security Planning Policy & Procedures (15 mins)

This infrastructure security course provides training to individuals with information security implementation and operational responsibilities for developing and disseminating an organization-wide security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance mapping.

Topics include:

- Establishing rules of behavior
- Security concept of operations
- Personnel security policies and procedures
- Position risk designations
- Personnel screening
- Access agreements

ENG 117 – Essential Information Security Program Planning (15 mins)

This infrastructure security course provides essential guidance to individuals with information security implementation and operational responsibilities on how to build and communicate an information security program plan to facilitate compliance with applicable regulatory requirements.

Topics include:

- Identifying information security resources
- Performing an information system inventory
- Creating a critical infrastructure plan
- Risk management strategy
- Insider threat program
- Training and developing contacts with security groups and associations

---

ENG 120 – Essential Security Assessment & Authorization (15 mins)

This infrastructure security course provides guidance for developing and implementing personnel security policies and associated controls to help ensure appropriate screening, on-boarding, and off-boarding of staff.

Topics include:

- Position risk designation
- Personnel screening and termination
- Personnel transfer and access agreement

ENG 126 – Essential Security Maintenance Policies (15 mins)

This infrastructure security course offers guidance to individuals with information security implementation and operational responsibilities for developing system maintenance procedures and controls.

Topics include:

- Controlled maintenance
- Maintenance tools
- Non-local maintenance
- Timely maintenance

ENG 212 – Implementing Secure Software Operations (20 mins)

All software activity involving critical assets must be tracked, and any methods that may expose sensitive data should also be tracked as defined by control objectives within the PCI Software Security Framework. Unfortunately, protecting the integrity of event datasets and analyzing records to detect attacks in real-time can be challenging. This course is designed to equip Information Systems Security Developers and Software Developers with the knowledge required to detect, respond to, and investigate attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet the Secure Software Operations requirements described in PCI's Secure Software Requirements and Assessment Procedures, including:

- Ensuring that all access attempts and usage of critical assets are tracked and traceable to a unique individual
- Facilitating the retention of detailed activity records either within the software itself or by supporting integration with other solutions such as centralized log servers, cloud-based logging solutions, or a back-end monitoring solution
- Ensuring that the software possesses the basic functionality to differentiate between normal and anomalous user behavior: such changes in post-deployment configurations or obvious automated-attack behaviors

---

ENG 312 – How to Perform a Security Code Review (30 mins)

Application developers have a variety of tools at their disposal to identify flaws in their software. However, many of them cannot be used until late in the development lifecycle: dynamic analysis tools require a staging site and sample data, and some static analysis tools require a compiled build. In contrast, manual code reviews can begin at any time leveraging secure coding knowledge. Because manual security code reviews can be laborious if done inefficiently, this course focuses on time saving but effective techniques.

Topics include:

- How to organize and approach code reviews
- Prioritizing code segments to be reviewed
- Maximizing security resources

Systems Requirements Planning (SRP)

COD 251 – Defending AJAX-Enabled Web Applications (25 mins)

This course introduces fundamentals of how to defend AJAX-enabled Web applications, including the difference between regular and AJAX-enabled web applications, AJAX security checks against challenges, and common attacks against AJAX-enabled applications.

Topics include:

- Architectural differences between regular web applications and AJAX-enabled applications
- Identifying threats to AJAX applications: cross-site scripting (XSS), cross-site request forgery (CSRF), and injection attacks
- Implementing countermeasures against attacks: protecting client resources, validating input, protecting web services requests, preventing request forgeries, and securing data access.

COD 253 – Creating Secure AWS Cloud Applications (45 mins)

This course examines the security vulnerabilities, threats, and mitigations for AWS cloud computing services and provides best practices for securing Web applications by leveraging AWS platform security features.

Topics include:

- AWS security features: Key Management Service (KMS), Hardware Security Module (HSM), Identity and Access Management (IAM), and CloudWatch
- How to leverage security features built into Common Amazon Cloud services such as Simple Storage Service (S3), Elastic Compute Cloud (Amazon EC2), Elastic Block Store (EBS), Amazon Glacier, Relational Database Service (RDS), DynamoDB, Elastic MapReduce (EMR), and Amazon Machine Images (AMI)

COD 254 – Creating Secure Azure Applications (45 mins)

This course examines key Azure security platforms and services that you can use to improve the security of your applications.

Topics include:

- Security vulnerabilities, threats, and mitigations for Azure cloud computing services
- How to identify common security threats to cloud-based applications
- Secure coding best practices to mitigate threats
- How to leverage built-in Azure features for an extra layer of defense

---

COD 255 – Creating Secure Code: Web API Foundations (20 mins)

This secure coding course introduces the fundamentals of secure web services development.

Topics include:

- Common web services threats that put your application at risk
- Impact of web services attacks
- Secure development best practices to protect web services

DES 101 – Fundamentals of Secure Architecture (20 mins)

In the past, software applications were created with little thought to the importance of security. Recently, businesses have become more rigorous about how they buy and deploy software as security is a large part of the total cost that risk software applications inherently carry. In this course, you examine the state of the industry from a security perspective, setting the foundation for secure software development.

Topics include:

- Application security architecture principles
- Lessons learned: security disasters in software design
- How to use confidentiality, integrity, and availability to drive better security design decisions

---

DES 260 – Fundamentals of IoT Architecture & Design (30 mins)

This course focuses on topics related to architecting and designing a secure Internet of Things (IoT) system. Particular emphasis is placed on embedded IoT devices and their relationship with cloud services.

After completing this course, you will have a deep understanding of an IoT system, its components, and the security implications of various design choices.

Topics include:

- Elements to be reviewed and defined in the requirements phase
- Authorization considerations within the IoT device itself as well as connected components
- Designing a secure IoT architecture
- Authentication to validate the identity of users and devices
- Logical access controls to ensure users are granted appropriate levels of service
- Physical security concerns to protect access to IoT devices
- Monitor communications throughout the IoT system
- Secure communications between the various system components

---

DES 306 – Creating a Secure Blockchain Network (20 mins)

While Blockchain technology continues to emerge for its ability to improve data security, speed up transactions and save costs, it comes with its advantages it comes with a wide array of challenges. Properly securing a blockchain network begins with the implementation of strong authentication and cryptography key vaulting mechanisms. This course provides learners with an understanding of the essential requirements for creating a secure blockchain network.

After completing this course you will be able to:

- Identify operational, legal and compliance requirements
- Create a blockchain threat model
- Create blockchain trust policies, access controls, and smart contracts
- Manage identity, access, entitlements, certificates, and keys
- Monitor, report, and manage incidents

DSO 253 – DevSecOps in the AWS Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course provides learners with an understanding of how to align and configure AWS services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Implement inventory and configuration controls and services, including AWS Config, AWS CloudFormation, and Amazon Inspector
- Ensure Infrastructure Security using Amazon VPC, AWS WAF, Customer-controlled encryption and automatic encryption of all traffic
- Mitigate DDoS threats with Autoscaling, Amazon CloudFront and Amazon Route 53
- Encrypt data using AWS Key Management Services (KMS), Server-side encryption (SSE), AWS CloudHSM; and leverage EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift encryption features
- Meet Monitoring and Logging requirements using AWS CloudTrail and Amazon CloudWatch
- Use Identity and Access Controls to define, enforce, and manage user access policies with AWS Identity and Access Management (IAM), AWS Multi-Factor Authentication and AWS Directory Services
- Understand AWS policies for customer Penetration Testing

DSO 254 – DevSecOps in the Azure Cloud (20 mins)

Using a cloud Platform solves issues with distributed complexity and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. Provides learners with an understanding of how to align and configure Azure services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

After completing this course you will be able to:

- Identify and manage the data, personnel, devices, systems, and facilities to meet the organization's business objectives and risk strategy
- Protect assets and associated facilities by using Access Control, limiting access to authorized users, processes, or devices, and to authorized activities and transactions
- Protect data-at-rest and data-in-transit by leveraging security services such as Azure Storage Service Encryption, Azure Backup Data Encryption, Azure SQL Transparent Data Encryption BitLocker, Azure VPN Gateway
- Detect anomalous activity in a timely manner and understand the potential impact of events by using Azure Security Center, Advanced Threat Analytics, Design and Implementation for Active Directory (DIAD), SIEM integration and Cloud App Security
- Ensure response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events

---

DSO 302- Automated Security Testing (20 mins)

Modern application development, increasing speed-to-market requirements, and assuring application security have made automated security testing a top priority for many organizations. Automating Security Testing can be difficult and daunting, but incorporating into workflows can provide consistency, expedience, and ensure software quality. This course teaches learners to integrate the built-in strengths of DevOps within the security Testing process while adhering to security testing needs.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Understanding the importance of orchestrating secure system and service configuration
- Determining which types of automated tests should be performed at various stages of the software development lifecycle
- Creating policies that support simultaneous testing and building in keeping with DevSecOps secure software development
- Leveraging Information Security Continuous Monitoring (ISCM) tools to perform a broad range of tasks, including periodic security and vulnerability scans of all system components

---

DSO 306 – Implementing Infrastructure as Code (20 mins)

Used to automate infrastructure deployment processes, Implementing Infrastructure as Code comes with a unique set of challenges making it hard for organizations to maintain agility, control, and visibility. This course is designed to help developers leverage Infrastructure as Code to securely and effectively launch cloud environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Using tools in the development stage to help convert requirements into source code
- Leveraging the security features available in most integrated development environments (IDEs) for multiple programming language support
- Identify and mitigate the most common IaC vulnerabilities, including Weak Authentication Tokens, Disclosure of Authentication Credentials, Excessive Privileges or Capabilities, Misconfigured Network Filtering, and Missing Encryption

---

DSO 307 – Secure Secrets Management (20 mins)

As the need to protect critical data increases, organizations must focus efforts on improving processes used to manage essential information. This course is designed to ensure software development teams employ appropriate techniques to manage identities, privileges, and secrets securely.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Ensuring that approved cryptographic algorithms and methods are used for securing critical assets
- Aligning key-management processes and procedures with those recognized by industry-standards bodies
- Using Approved Random Number Generators| Providing strong entropy when Using Random Number Generator

ENG 114 – Essential Risk Assessment (15 mins)

This infrastructure security course provides essential guidance on information system risk assessment techniques. Individuals responsible for information systems, IT security, risk management, or oversight responsibilities will find this course valuable. It teaches how to define and manage the purpose, scope, roles, and coordination among organizational entities to help ensure appropriate risk assessment and compliance with applicable regulatory requirements.

Topics include:

- Security categorization
- Risk assessment
- Vulnerability scanning
- The system development lifecycle
- Security engineering principles
- Developer security testing and evaluation
- Development process, standards, and tools
- Developer security architecture and design
- Component authenticity

ENG 115 – Essential System & Information Integrity (15 mins)

This infrastructure security course provides essential guidance to program managers, system designers and developers on how to identify systems affected by software flaws, assess potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel.

Topics include:

- Flaw remediation
- Malicious code protection
- Information system monitoring
- Software, firmware, and information integrity
- Information input validation
- Error handling
- Information handling and retention
- Information output filtering
- Memory protection

ENG 116 – Essential Security Planning Policy & Procedures (15 mins)

This infrastructure security course provides training to individuals with information security implementation and operational responsibilities for developing and disseminating an organization-wide security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance mapping.

Topics include:

- Establishing rules of behavior
- Security concept of operations
- Personnel security policies and procedures
- Position risk designations
- Personnel screening
- Access agreements

ENG 117 – Essential Information Security Program Planning (15 mins)

This infrastructure security course provides essential guidance to individuals with information security implementation and operational responsibilities on how to build and communicate an information security program plan to facilitate compliance with applicable regulatory requirements.

Topics include:

- Identifying information security resources
- Performing an information system inventory

- Creating a critical infrastructure plan
- Risk management strategy
- Insider threat program
- Training and developing contacts with security groups and associations

---

ENG 120 – Essential Security Assessment & Authorization (15 mins)

This infrastructure security course provides guidance for developing and implementing personnel security policies and associated controls to help ensure appropriate screening, on-boarding, and off-boarding of staff.

Topics include:

- Position risk designation
- Personnel screening and termination
- Personnel transfer and access agreement

ENG 123 – Essential Security Engineering Principles (15 mins)

This infrastructure security course provides direction to program managers, system designers, developers, information security engineers, and systems integrators responsible for new information systems development or systems undergoing major upgrades.

Topics include:

- System development life cycle
- Developer security testing and evaluation
- Development process, standards, and tools
- Developer security architecture
- Design and component authenticity

ENG 124 – Essential Application Protection (15 mins)

This infrastructure security course imparts guidance to system designers and developers on implementing specific security controls at the software level to protect applications and comply with applicable regulatory requirements.

Topics include:

- Implementing defense-in-depth
- Separation of system and user functionality
- Securing components
- Validating input
- Encoding output

ENG 126 – Essential Security Maintenance Policies (15 mins)

This infrastructure security course offers guidance to individuals with information security implementation and operational responsibilities for developing system maintenance procedures and controls.

Topics include:

- Controlled maintenance
- Maintenance tools
- Non-local maintenance
- Timely maintenance

ENG 191 – Introduction to the Microsoft SDL (25 mins)

This course introduces the industry-leading Microsoft Security Development Lifecycle (SDL) Optimization Model and how to implement it.

Topics include:

- Capability areas of the Microsoft SDL Optimization Model
- Maturity levels and how to reach them
- Optimization techniques to reduce risk

ENG 192- Implementing the Agile Microsoft SDL (20 mins)

The standard MS SDL process follows the traditional incremental waterfall model, while Agile methodologies are more iterative. This course focuses on the Agile variation of the SDL process and covers the following topics:

- How to map critical SDL security practices into every-sprint requirements, bucket or periodic requirements, and one-time requirements
- How to incorporate security education, tooling and automation, threat modeling, fuzz testing, handling bug-dense and at-risk code, exceptions, and the final security review into sprints

---

ENG 193 – Implementing the Microsoft SDL Optimization Model (12 mins)

This course describes the main phases of the Microsoft Security Development Lifecycle (SDL) process: Requirements, Design, Implementation, Verification, and Release, with a focus on security throughout.

After completing this course, you will have a solid understanding of the SDL process and the recommended/required tasks for each phase.

ENG 194 – Implementing Microsoft SDL Line of Business (20 mins)

This course describes the Microsoft Security Development Lifecycle for Line of Business (SDL-LOB), which focuses on the development of internal or business-facing applications.

Topics include:

- The five primary phases of the SDL: Requirements, Design, Implementation, Verification, and Release
- LOB-specific tasks, requirements and deliverables for each phase of the SDL
- How to integrate security-improving tasks at each level of risk
- Necessary skills to be effective

ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)

This course describes the features of the Microsoft SDL Threat Modeling tool, which complements the Microsoft SDL Threat Modeling process. While not required to perform threat modeling, using the tool facilitates the creation of threat models and helps enumerate threats using STRIDE.

Topics include:

- Creating accurate data flow diagrams (DFDs) in your threat model
- Identifying flaws in DFDs and analyzing it for potential threats
- Generating reports to export threats to issue tracking tools

---

ENG 205 – Fundamentals of Threat Modeling (45 mins)

This course describes how to take a question-driven approach to threat modeling to help identify security design problems early in development process.

After completing this course, you will be able to create a threat model for your application scenario and use it to refine your application's design and improve communication within the team.

ENG 212 – Implementing Secure Software Operations (20 mins)

All software activity involving critical assets must be tracked, and any methods that may expose sensitive data should also be tracked as defined by control objectives within the PCI Software Security Framework. Unfortunately, protecting the integrity of event datasets and analyzing records to detect attacks in real-time can be challenging. This course is designed to equip Information Systems Security

Developers and Software Developers with the knowledge required to detect, respond to, and investigate attacks.

Upon successful completion of this course, learners will have the knowledge and skills required to meet the Secure Software Operations requirements described in PCI's Secure Software Requirements and Assessment Procedures, including:

- Ensuring that all access attempts and usage of critical assets are tracked and traceable to a unique individual
- Facilitating the retention of detailed activity records either within the software itself or by supporting integration with other solutions such as centralized log servers, cloud-based logging solutions, or a back-end monitoring solution
- Ensuring that the software possesses the basic functionality to differentiate between normal and anomalous user behavior: such changes in post-deployment configurations or obvious automated-attack behaviors

---

TST 101 – Fundamentals of Security Testing (20 mins)

This course introduces security testing concepts and processes that will help testers/QA teams analyze an application from a security perspective to conduct more effective security testing.

Topics include:

- Classes of security vulnerabilities and testing approaches that target them
- Manual and automated test techniques
- Identifying common security issues
- Threat modeling, approaches and how they apply to the design phase of the SDLC
- Vulnerability scanning, penetration testing, static analysis, and code review

---

TST 205 – Performing Vulnerability Scans (45 mins)

Performing vulnerability scans is a necessary first step to evaluating the security of an organization's network and helping protect organizational data and assets; this includes assessing, mitigating, and reporting on any security vulnerabilities that exist in an organization's systems and software.

Topic includes:

- Enumerating Platforms, Software Flaws, and improper configurations
- Formatting Checklists and test procedures
- Measuring vulnerability impact
- Analyzing vulnerability scan reports and results from security control assessments

---

Targets (TGT)

DSO 211 – Identifying Threats to Containers in a DevSecOps Framework (20 mins)

Widespread adoption of cloud computing and DevOps have led to containers becoming the most popular and efficient way to deploy applications. However, containerization presents enterprise security risks that question existing security policies and compliance frameworks. This course provides a necessary understanding of known attacks required to improve the security of container application deployments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- The importance of Identifying threats to containers and data in the DevSecOps framework
- Why containers are particularly susceptible to image vulnerabilities, and how to mitigate the threat by rebuilding images as part of security updates.
- How to validate external images to prevent malware, unintended functionality, functional bugs, or components with known vulnerabilities into your environment
- Securely encrypting communication channels to avoid man-in-the-middle attacks designed to extract image contents, compromise credentials used to access registries or tamper with images being sent to orchestrators

---

Technology R&D (TRD)

DES 306 – Creating a Secure Blockchain Network (20 mins)

While Blockchain technology continues to emerge for its ability to improve data security, speed up transactions and save costs, it comes with its advantages it comes with a wide array of challenges. Properly securing a blockchain network begins with the implementation of strong authentication and cryptography key vaulting mechanisms. This course provides learners with an understanding of the essential requirements for creating a secure blockchain network.

After completing this course you will be able to:

- Identify operational, legal and compliance requirements
- Create a blockchain threat model
- Create blockchain trust policies, access controls, and smart contracts
- Manage identity, access, entitlements, certificates, and keys
- Monitor, report, and manage incidents

Test and Evaluation (TST)

COD 170 – Identifying Threats to Mainframe COBOL Applications & Data (20 mins)

This secure coding course covers the most common security issues that affect the confidentiality, integrity and availability of COBOL programs on mainframes. These include SQL Injection, Command Injection, Integer Overflow, Weak Cryptography, Unencrypted Communications and Race Conditions.

COD 249 – PCI DSS 11: Regularly Test Security Systems and Processes (15 mins)

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software, system components, and custom software. The software should be tested regularly to ensure security controls continue to reflect a changing environment.

In this course, you will learn how to ensure critical data can only be accessed by authorized personnel and develop an understanding of systems and processes that must be in place to limit access based on a need to know and according to job responsibilities. Additionally, you will learn how to test security controls and ensure they continue to reflect a changing environment.

COD 383 – Protecting Java Backend Services (30 mins)

Backends are designed for applications that need faster performance, large amounts of addressable memory, and continuous or long-running background processes. The versatility of Java enables developers to design and deliver the right business solutions however their efficiency requires distinctive experiencer and great expertise.

This course aims to provide software developers and DevOps Engineers with the next level understanding of best practices for developing back end frameworks using Java while developing skills necessary to handle user input and build secure systems.

Topics Include:

- The Function of OAuth2 and JWT
- How to leverage the JAAS API
- The advantages of the Spring Security framework
- Validating Length Before Applying RegEx
- Protecting Sensitive Data in Transit Using TLS
- How to identify and protect against SQLi, HQLi, XXE, CSRF, and RegEx DoS attacks

---

CYB 301 – Fundamentals of Ethical Hacking (15 mins)

As hackers continue to evolve their techniques organizations must train their employees to test their defenses through various penetration techniques. This course introduces common activities performed during the process of Ethical Hacking and provides a basic foundation of common attack techniques and examples of hacking tools.

Topics Include:

- Understanding authorization and scope that define ethical hacking

- Implementing the penetration testing process
- Fundamentals of attacker techniques and the ATT& CK framework
- An overview of hacking skills and tools knowledge domain

DSO 302- Automated Security Testing (20 mins)

Modern application development, increasing speed-to-market requirements, and assuring application security have made automated security testing a top priority for many organizations. Automating Security Testing can be difficult and daunting, but incorporating into workflows can provide consistency, expedience, and ensure software quality. This course teaches learners to integrate the built-in strengths of DevOps within the security Testing process while adhering to security testing needs.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Understanding the importance of orchestrating secure system and service configuration
- Determining which types of automated tests should be performed at various stages of the software development lifecycle
- Creating policies that support simultaneous testing and building in keeping with DevSecOps secure software development
- Leveraging Information Security Continuous Monitoring (ISCM) tools to perform a broad range of tasks, including periodic security and vulnerability scans of all system components

---

ENG 195 – Implementing the Microsoft SDL Threat Modeling Tool (20 mins)

This course describes the features of the Microsoft SDL Threat Modeling tool, which complements the Microsoft SDL Threat Modeling process. While not required to perform threat modeling, using the tool facilitates the creation of threat models and helps enumerate threats using STRIDE.

Topics include:

- Creating accurate data flow diagrams (DFDs) in your threat model
- Identifying flaws in DFDs and analyzing it for potential threats
- Generating reports to export threats to issue tracking tools

---

ENG 205 – Fundamentals of Threat Modeling (45 mins)

This course describes how to take a question-driven approach to threat modeling to help identify security design problems early in development process.

After completing this course, you will be able to create a threat model for your application scenario and use it to refine your application's design and improve communication within the team.

TST 101 – Fundamentals of Security Testing (20 mins)

This course introduces security testing concepts and processes that will help testers/QA teams analyze an application from a security perspective to conduct more effective security testing.

Topics include:

- Classes of security vulnerabilities and testing approaches that target them
- Manual and automated test techniques
- Identifying common security issues
- Threat modeling, approaches and how they apply to the design phase of the SDLC
- Vulnerability scanning, penetration testing, static analysis, and code review

---

TST 205 – Performing Vulnerability Scans (45 mins)

Performing vulnerability scans is a necessary first step to evaluating the security of an organization's network and helping protect organizational data and assets; this includes assessing, mitigating, and reporting on any security vulnerabilities that exist in an organization's systems and software.

Topic includes:

- Enumerating Platforms, Software Flaws, and improper configurations
- Formatting Checklists and test procedures
- Measuring vulnerability impact
- Analyzing vulnerability scan reports and results from security control assessments

---

Vulnerability Assessment and Management (VAM)

ATK 201 – Using the MITRE ATT&CK Framework (15 mins)

The MiTRE ATT& CK Framework is a knowledge base of globally observed adversary tactics and techniques. This course provides an understanding of behaviors that may be used for developing threat models, mapping threats, classifying attacks, or training both red and blue teams.

Topics Include:

- The purpose of the ATT&CK Framework
  Structures, tactics, and techniques within the framework
- Using the ATT&CK Framework to detect and analyze threats
- Mitigation best-practices for preventing attacks

DSO 301 – Orchestrating Secure System and Service Configuration (20 mins)

Building and maintaining quality software requires functional configuration management, but this is easier said than done in today's day and age. This process involves automation, but minimizing errors while securely and systematically managing changes in systems is complicated. This course provides Systems Developers, Network Operations Specialists, System Administrators, and Systems Security Analysts with the necessary skills to consistently and securely manage environments.

Upon successful completion of this course, learners will have the knowledge and skills required to meet compliance requirements while developing a DevSecOps mindset, including:

- Identifying and mitigating gaps in your current orchestration security policies
- Ensuring the coordination and consistency of security policies across the enterprise
- The importance of maintaining immutability of live container instances, ensuring that changes occur in the source control and are only deployed via new versions of the resource
- Understanding the role of third-party tools such as Clair, Actuary, and Anchore in testing Infrastructure-as-Code (IAC) and Configuration-as-Code (CAC) platforms

---

ENG 211 – How to Create Application Security Design Requirements (15 mins)

To preserve the confidentiality, integrity, and availability of application data, software applications must be engineered with security in mind. Without defined security requirements, design choices will be made without security guidance and security testing cannot be effective.

This course provides technical and non-technical personnel with the knowledge to understand, create, and articulate security requirements as part of a software requirement document.

Topics include:

- Applying the application security maturity (ASM) model to the development process
- Key security engineering activities: gathering security objectives, applying security design guidelines, and creating threat models
- Identifying threats, attacks, vulnerabilities, and countermeasures
- How to conduct impactful security architecture and design reviews to identify potential security problems and minimize the application's attack surface.

ENG 311 – Attack Surface Analysis & Reduction (25 mins)

The attack surface of an application represents the number of entry points exposed to a potential attacker. The larger the attack surface, the larger the set of methods that can be used by an adversary breaking into software applications. Resultantly, minimizing it is a key exercise in risk reduction.

Topics covered:

- Understanding the goals and methodologies of attackers
- Identifying attack vectors that expose the application
- Defining and reducing an application's attack surface

TST 202 – Penetration Testing Fundamentals (25 mins)

Serving as a comprehensive way of testing for cybersecurity vulnerabilities Penetration Testing provides insight into a network, application, device, and/or physical security through the lens of an attacker to discover weaknesses and identify areas of improvement within your security posture. This course introduces concepts of penetration testing and provides an understanding of the stages of penetration testing as they relate to industry standards.

After completing this course, you will be able to:

- Conduct penetration testing according to an industry-standard methodology
- Identify the steps in a typical penetration testing process

---

TST 301 – Infrastructure Penetration Testing (45 mins)

Reliance on IT systems, regulatory compliance, and the evolving cyberthreat landscape are key indicators of the importance of Infrastructure penetration testing. Infrastructure Penetration tests can help inform cybersecurity strategies, validate existing security controls, and identify weaknesses in need of improvement. This course provides learners with the skills and knowledge necessary to perform penetration tests that simulate how attackers might attempt to compromise the organization's infrastructure.

After completing this course you will be able to:

- Perform pretest identification of potential vulnerabilities based on pretest analysis
- Leverage automated scanning tools
- Establish a baseline indication of the potential attack surface of the environment
- Interpret the results of automated tools to determine what additional testing is needed
- Perform host discovery, port scanning, and network segmentation checks
- Analyze the results of the penetration test are then compiled into a report

---

TST 302 – Application Penetration Testing (45 mins)

Applications store, process, and transmit data making them susceptible and vulnerable to hackers who can identify and exploit vulnerabilities. Penetration testing of these applications acts as a safeguard to reduce vulnerabilities and attack surface. This course provides learners with the skills and knowledge necessary to perform penetration tests that simulate how attackers might attempt to compromise the software applications.

After completing this course you will be able to:

- Conduct planning and reconnaissance
- Scan to understand how the target application will respond to various intrusion attempts
- Gain access using web application attacks, such as cross-site scripting, SQL injection, and backdoors, to uncover a target's vulnerabilities
- Maintain access to determine if the vulnerability can be used to achieve a persistent presence in the exploited system
- Analyze the results of the penetration test are then compiled into a report

---

TST 351 – Penetration Testing for TLS Vulnerabilities (12 mins)

The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. However, flaws in TLS protocol include weak cryptographic primitives, or specific implementation errors, cross-protocol vulnerabilities, or any combination of each. This course teaches how to identify vulnerabilities, detecting acceptance of unencrypted connections, and testing configurations.

After completing this course, you will be able to:

- Identify typical TLS misconfiguration vulnerabilities
- Detect network services accepting unencrypted connections
- Test web server TLS configuration

TST 352 – Penetration Testing for Injection Vulnerabilities (12 mins)

Stemming from improperly sanitized or completely unsensitized input injection flaws allow attackers to relay malicious code through an application to another system. This course teaches how to identify and test for these vulnerabilities within your code.

After completing this course, you will be able to:

- Identify common injection vulnerabilities
- Test for command injection vulnerabilities
- Detect code and XML injection vulnerabilities
- Exploit command and code injection vulnerabilities

TST 353 – Penetration Testing for SQL Injection (12 mins)

Used to attack data-driven applications in which malicious SQL statements are inserted into an entry field for execution SQL Injection allows attackers to conduct a number of malicious activities to data including but not limited to becoming administrators of the database server. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Test for the presence of SQL Injection vulnerabilities
- Exploit SQL Injection vulnerabilities
- Identify the common tools and techniques used to exploit SQL Injection vulnerabilities

---

TST 354 – Penetration Testing for Memory Corruption Vulnerabilities (12 mins)

Occurring when the contents of a memory location are modified due to programmatic behavior that exceeds the intention of the original programmer or program/language constructs. This type of programming error can lead to a program crash or strange and bizarre program behavior. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Identify common memory corruption vulnerabilities
- Test for buffer overflows + Exploit known memory corruption vulnerabilities
- Understand advanced techniques for finding memory corruption vulnerabilities

---

TST 355 – Penetration Testing for Authorization Vulnerabilities (12 mins)

Authorization is the process of enforcing policies; determining what types of qualities of activities, resources, or services a user is permitted. Authorization vulnerabilities include forceful browsing and privilege escalation. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Identify common authorization vulnerabilities
- Test application access controls
- Exploit authorization vulnerabilities

TST 356 – Penetration Testing for Cross-Site Scripting (XSS) (12 mins)

Cross-site Scripting (XSS) is a client-side code injection attack where the attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. This course teaches how to identify, test, and exploit these vulnerabilities.

After completing this course, you will be able to:

- Define the types of Cross-Site Scripting vulnerabilities

- Test applications for Cross-Site Scripting vulnerabilities
- Exploit Cross-Site Scripting vulnerabilities

TST 357 – Penetration Testing for Hardcoded Secrets (12 mins)

All modern applications rely on certain secrets to run from database connection strings to API keys or cryptographic keys. Keeping these secrets is critical to the security of the application as they typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This course teaches how to identify and test for the use of hard-coded credentials.

After completing this course, you will be able to:

- Determine whether an application contains hard-coded authentication credentials
- Determine whether an application contains hard-coded cryptographic keys
- Find plain-text secrets in application binaries
- Find leaked secrets in code repositories
- Identify techniques for advanced testing of application code for the presence of hard-coded secrets

---

TST 358 – Penetration Testing Wireless Networks (12 mins)

Wireless networks have security issues that are vulnerable to various attacks. Organizations need to proactively search out any weakness in security if they are to avoid unauthorized access to network resources and data leakage. This course introduces tools and techniques while teaching how to Identify and test for common attacks.

After completing this course, you will be able to:

- Test for the presence of unauthorized wireless networks
- Identify common attacks on wireless networks
- Identify the common tools and techniques for testing wireless networks

---

TST 359 – Penetration Testing Network Infrastructure (12 mins)

Essential to every organization; Infrastructure penetration testing provides an opportunity to know about the current situation of a company and analyze existing potential breach points. The process includes all internal computer systems, associated external devices, internet networking, cloud, and virtualization testing. This course teaches how to perform Network Infrastructure penetration tests, perform necessary scans, and test controls.

After completing this course, you will be able to:

- Perform network-layer penetration tests
- Test network segmentation controls
- Perform a network scan to discover active devices
- Perform a port scan on a host to identify exposed network services

---

TST 360 – Penetration Testing for Authentication Vulnerabilities (12 mins)

Building authentication and session management schemes correctly is a difficult task often presenting flaws that may equally difficult to Identify. Common authentication attacks consist of brute force, insufficient authentication, and weak password recovery validation. These types of attacks target and attempt to exploit the authentication process a web site uses to verify the identity of a user, service, or application. This course teaches how to execute attacks, identify vulnerabilities, and verify controls.

After completing this course, you will be able to:

- Identify common authentication vulnerabilities
- Verify authentication controls
- Execute dictionary attacks

Contact Us
187 Ballardvale Street, Suite A195
Wilmington, MA 01887
Phone: +1.877.839.7598