

**SECURITY
INNOVATION**

Training Program Catalog

eLearning

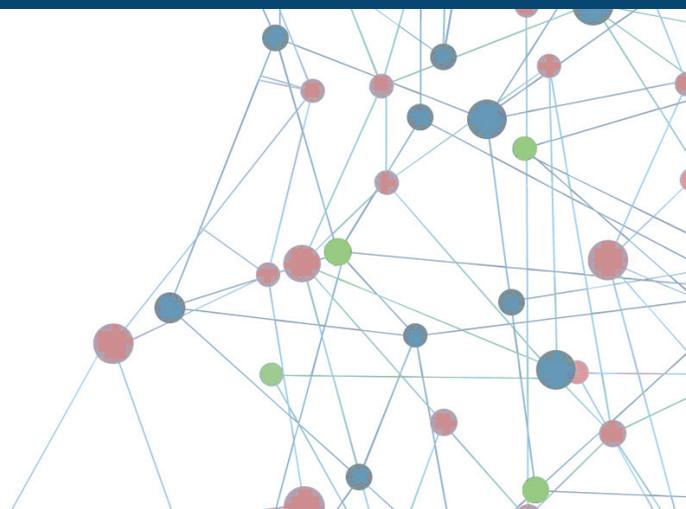
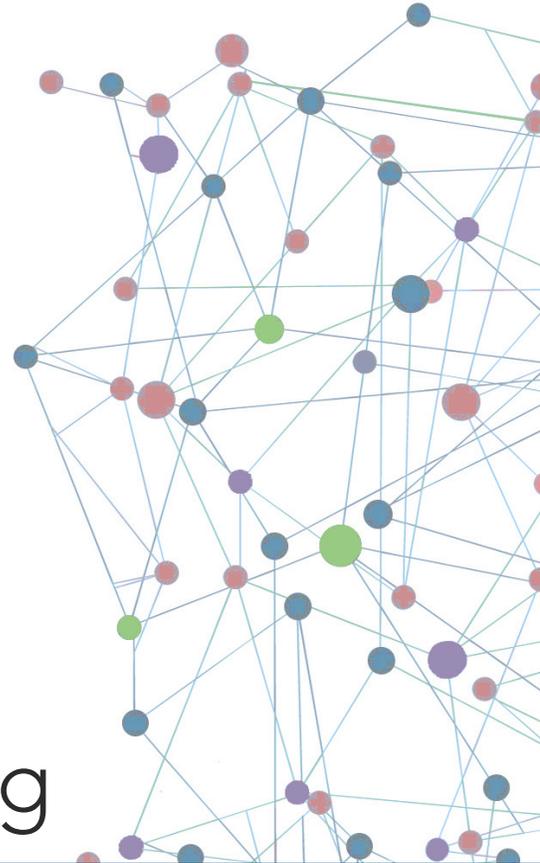


Table of Contents

Computer Based Training - Security Awareness - General Staff

AWA 007 - Information Privacy and Security Awareness for Executives (Duration: 45 minutes).....	1
AWA 008 - Information Privacy - Classifying Data (Duration: 15 minutes).....	1
AWA 009 - Information Privacy - Protecting Data (Duration: 20 minutes).....	1
AWA 010 - Email Security (Duration: 10 minutes).....	1
AWA 012 - Malware Awareness (Duration: 10 minutes).....	1
AWA 013 - Mobile Security (Duration: 15 minutes).....	1
AWA 014 - Password Security (Duration: 10 minutes).....	2
AWA 015 - PCI Compliance (Duration: 15 minutes).....	2
AWA 016 - Phishing Awareness (Duration: 10 minutes).....	2
AWA 017 - Physical Security (Duration: 10 minutes).....	2
AWA 018 - Social Engineering Awareness (Duration: 15 minutes).....	2
AWA 019 - Travel Security (Duration: 15 minutes).....	2

Computer Based Training - Secure Coding

AWA 101 - Fundamentals of Application Security (Duration: 60 minutes).....	3
AWA 102 - Secure Software Concepts (NEW Duration: 30 minutes).....	3
COD 101 - Fundamentals of Secure Development (Duration: 60 minutes).....	3
COD 110 - Fundamentals of Secure Mobile Development (Duration: 60 minutes).....	3
COD 141 - Fundamentals of Secure Database Development (Duration: 110 minutes).....	3
COD 152 - Fundamentals of Secure Cloud Development (Duration: 30 minutes).....	4
COD 153 - Fundamentals of Secure AJAX Code (Duration: 35 minutes).....	4
COD 160 - Fundamentals of Secure Embedded Software Development (Duration: 90 minutes).....	4
COD 170 - Identifying Threats to Mainframe COBOL Applications and Data (Duration: 20 minutes).....	4
COD 200 - Creating Secure C Code Series	4
COD 201 - Secure C Encrypted Network Communications (Duration: 15 minutes).....	4
COD 202 - Secure C Run-Time Protection (Duration: 15 minutes).....	5
COD 205 - Creating Secure C++ Code Series (Duration: 55 minutes).....	5
COD 206 - Creating Secure C++ Code (Duration: 15 minutes).....	5
COD 207 - Communication Security in C++ (Duration: 15 minutes).....	5
COD 307 - Protecting Data in C++ (NEW Duration: 25 minutes).....	5
COD 215 - Creating Secure Code .NET Framework Foundations Series (NEW)	6
COD 216 - Leveraging .NET Framework Code Access Security (CAS) (NEW Duration: 30 minutes).....	6
COD 217 - Mitigating .NET Security Threats (NEW Duration: 45 minutes).....	6
COD 219 - Creating Secure Code - SAP ABAP Foundations (Duration: 90 minutes).....	6
COD 222 - PCI DSS v3.2 Best Practices for Developers (Duration: 60 minutes).....	6
COD 224 - IoT Specialization Series	6
COD 225 - Insecure IoT Web Interfaces (Duration: 10 minutes).....	7
COD 226 - Insecure IoT Authentication and Authorization (Duration: 10 minutes).....	7
COD 227 - Insecure IoT Network Services (Duration: 10 minutes).....	7
COD 228 - Insecure IoT Communications (Duration: 10 minutes).....	7
COD 229 - Insecure IoT Mobile Interface (Duration: 10 minutes).....	7
COD 230 - Insecure IoT Firmware (Duration: 10 minutes).....	7
COD 233 - OWASP Mobile Series	7
COD 234 - Mobile Threats and Mitigations (Duration: 20 minutes).....	8
COD 235 - Defending Mobile Data with Cryptography (Duration: 20 minutes).....	8
COD 236 - Mobile App Authentication and Authorization (Duration: 20 minutes).....	8
COD 237 - Defending Mobile App Code (Duration: 20 minutes).....	8
COD 241 - Creating Secure Oracle Database Applications (NEW Duration: 45 minutes).....	8
COD 242 - Creating Secure SQL Server and Azure SQL Database Applications (Duration: 40 minutes).....	8
COD 251 - Creating Secure AJAX Code - ASP.NET Foundations (Duration: 90 minutes).....	8
COD 252 - Creating Secure AJAX Code - Java Foundations (Duration: 35 minutes).....	9
COD 253 - Creating Secure AWS Cloud Applications (Duration: 60 minutes).....	9
COD 254 - Creating Secure Azure Applications (Duration: 90 minutes).....	9
COD 255 - Creating Secure Code - Web API Foundations (Duration: 120 minutes).....	9
COD 256 - Creating Secure Code - Ruby on Rail Foundations (Duration: 90 minutes).....	9
COD 257 - Creating Secure Python Web Applications (Duration: 45 minutes).....	10
COD 259 - Node.js Threats and Vulnerabilities (NEW Duration: 30 minutes).....	10
COD 260 - Secure Scripting Series	10
COD 261 - Threats to Scripts (Duration: 30 minutes).....	10
COD 262 - Fundamentals of Secure Scripting (Duration: 30 minutes).....	10

COD 263 - Secure Scripting with Perl, Python, Bash and Ruby (Duration: 30 minutes).....	10
COD 264 - Protecting Sensitive Data while Scripting (Duration: 30 minutes)	11
COD 270 - Creating Secure COBOL and Mainframe Applications (Duration: 25 minutes)	11
COD 280 - Creating Secure Java Series	11
COD 281 - Java Security Model (Duration: 20 minutes)	11
COD 282 - Java Authentication and Authorization (JAAS) (Duration: 20 minutes).....	11
COD 283 - Java Cryptography (Duration: 30 minutes)	11
COD 300 - Protecting C Code Series	12
COD 301 - Secure C Buffer Overflow Mitigations (Duration: 45 minutes)	12
COD 302 - Secure C Memory Management (Duration: 30 minutes)	12
COD 303 - Common C Vulnerabilities and Attacks (Duration: 20 minutes)	12
COD 311 - Creating Secure Code ASP.NET MVC Applications (Duration: 90 minutes).....	12
COD 315 - Creating Secure PHP Code (Duration: 120 minutes).....	12
COD 316 - Creating Secure iOS Code in Objective C (Duration: 30 minutes)	13
COD 317 - Creating Secure iOS Code in Swift (Duration: 90 minutes).....	13
COD 318 - Creating Secure Android Code in Java (Duration: 90 minutes).....	13
COD 320 - Protecting C# Series (NEW)	13
COD 321 - Protecting C# from Integer Overflows and Canonicalization Issues (NEW Duration: 30 minutes)	13
COD 322 - Protecting C# from SQL and XML Injection (NEW Duration: 35 minutes).....	13
COD 323 - Protecting Data in C# (NEW Duration: 25 minutes).....	14
COD 352 - Creating Secure jQuery Code (Duration: 90 minutes).....	14
COD 360 - Creating Secure HTML5 Code Series (NEW)	14
COD 361 - HTML5 Security Threats (NEW Duration: 15 minutes)	14
COD 362 - HTML5 Built-In Security Features (NEW Duration: 20 minutes)	14
COD 363 - Securing HTML5 Data (NEW Duration: 20 minutes).....	14
COD 364 - Securing HTML5 Connectivity (NEW Duration: 20 minutes).....	15
COD 379 - Protecting Java Code Series (NEW)	15
COD 380 - Protecting Java Code: SQLi and Integer Overflows (NEW Duration: 10 minutes)	15
COD 381 - Protecting Java Code: Canonicalization, Information Disclosure and TOCTOU (NEW Duration: 25 minutes).....	15
COD 382 - Protecting Data in Java (NEW Duration: 30 minutes)	15

Computer Based Training - Secure Design

DES 101 - Fundamentals of Secure Architecture (Duration: 60 minutes).....	16
DES 201 - Fundamentals of Cryptography Series (NEW)	16
DES 202 - Cryptographic Suite Services: Encoding, Encrypting and Hashing (NEW Duration: 45 minutes)	16
DES 203 - Cryptographic Components: Randomness, Algorithms, and Key Management (NEW Duration: 15 minutes).....	16
DES 204 - The Role of Cryptography in Application Development (NEW Duration: 15 minutes)	16
DES 205 - Message Integrity Cryptographic Functions (NEW Duration: 45 minutes)	17
DES 212 - Architecture Risk Analysis and Remediation (Duration: 60 minutes)	17
DES 213 - Secure Enterprise Infrastructure Series	17
DES 214 - Securing Network Access (Duration: 30 minutes).....	17
DES 215 - Securing Operating System Access (Duration: 30 minutes).....	17
DES 216 - Securing Cloud Instances (Duration: 30 minutes)	17
DES 217 - Application, Technical and Physical Access Controls (Duration: 30 minutes).....	18
DES 221 - OWASP 2017 Series	18
DES 222 - Applying OWASP 2017: Mitigating Injection (Duration: 12 minutes).....	18
DES 223 - Applying OWASP 2017: Mitigating Broken Authentication (Duration: 12 minutes)	18
DES 224 - Applying OWASP 2017: Mitigating Sensitive Data Exposure (Duration: 12 minutes).....	18
DES 225 - Applying OWASP 2017: Mitigating XML External Entities (XXE) (Duration: 12 minutes).....	18
DES 226 - Applying OWASP 2017: Mitigating Broken Access Control (Duration: 12 minutes)	18
DES 227 - Applying OWASP 2017: Mitigating Security Misconfiguration (Duration: 12 minutes).....	18
DES 228 - Applying OWASP 2017: Mitigating Cross Site Scripting (XSS) (Duration: 12 minutes).....	19
DES 229 - Applying OWASP 2017: Mitigating Insecure Deserialization (Duration: 12 minutes).....	19
DES 230 - Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities (Duration: 12 minutes)	19
DES 231 - Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities (Duration: 12 minutes)	19
DES 260 - Fundamentals of IoT Architecture and Design (NEW Duration: 30 minutes).....	19
DES 311 - Creating Secure Application Architecture (Duration: 120 minutes).....	19
DES 352 - Creating Secure Over the Air (OTA) Automotive System Updates (Duration: 90 minutes).....	19

Computer Based Training - Secure Engineering

ENG 190 - Implementing the MS SDL Process Into your SDLC Series (NEW)	20
ENG 191 - Introduction to the Microsoft SDL (NEW Duration: 25 minutes)	20
ENG 192 - Implementing the Agile MS SDL (NEW Duration: 20 minutes).....	20
ENG 193 - Implementing the MS SDL Optimization Model (NEW Duration: 12 minutes).....	20
ENG 194 - Implementing MS SDL Line of Business (NEW Duration: 20 minutes).....	20

ENG 195 - Implementing the MS SDL Threat Modeling Tool (NEW Duration: 20 minutes).....	20
ENG 205 - Fundamentals of Threat Modeling (Duration: 60 minutes).....	21
ENG 211 - How to Create Application Security Design Requirements (Duration: 60 minutes).....	21
ENG 311 - Attack Surface Analysis & Reduction (Duration: 60 minutes).....	21
ENG 312 - How to Perform a Security Code Review (Duration: 60 minutes).....	21

Computer Based Training - Secure Testing

TST 101 - Fundamentals of Security Testing (Duration: 120 minutes).....	22
TST 221 - Testing for OWASP 2017 Series (NEW)	22
TST 222 - Testing for OWASP 2017: Injection (NEW Duration: 15 minutes).....	22
TST 223 - Testing for OWASP 2017: Broken Authentication (NEW Duration: 12 minutes).....	22
TST 224 - Testing for OWASP 2017: Sensitive Data Exposure (NEW Duration: 12 minutes).....	22
TST 225 - Testing for OWASP 2017: XML External Entities (NEW Duration: 10 minutes).....	23
TST 226 - Testing for OWASP 2017: Broken Access Control (NEW Duration: 10 minutes).....	23
TST 227 - Testing for OWASP 2017: Security Misconfiguration (NEW Duration: 10 minutes).....	23
TST 228 - Testing for OWASP 2017: Cross Site Scripting (NEW Duration: 15 minutes).....	23
TST 229 - Testing for OWASP 2017: Insecure Deserialization (NEW Duration: 10 minutes).....	23
TST 230 - Testing for OWASP 2017: Use of Components with Known Vulnerabilities (NEW Duration: 10 minutes).....	24
TST 231 - Testing for OWASP 2017: Insufficient Logging and Monitoring (NEW Duration: 10 minutes).....	24
TST 250 - Testing for CWE SANS Top 25 Software Errors Series (NEW)	24
TST 251 - Testing for SQL Injection (NEW Duration: 15 minutes).....	24
TST 252 - Testing for OS Command Injection (NEW Duration: 15 minutes).....	24
TST 253 - Testing for Classic Buffer Overflow (NEW Duration: 15 minutes).....	25
TST 254 - Testing for Cross-site Scripting (NEW Duration: 15 minutes).....	25
TST 255 - Testing for Missing Authentication for Critical Function (NEW Duration: 15 minutes).....	25
TST 256 - Testing for Missing Authorization (NEW Duration: 15 minutes).....	25
TST 257 - Testing for Use of Hard-Coded Credentials (NEW Duration: 15 minutes).....	25
TST 258 - Testing for Missing Encryption of Sensitive Data (NEW Duration: 15 minutes).....	26
TST 259 - Testing for Unrestricted Upload of File with Dangerous Type (NEW Duration: 15 minutes).....	26
TST 260 - Testing for Reliance on Untrusted Inputs in a Security Decision (NEW Duration: 15 minutes).....	26
TST 261 - Testing for Execution with Unnecessary Privileges (NEW Duration: 15 minutes).....	26
TST 262 - Testing for Cross Site Request Forgery (NEW Duration: 15 minutes).....	26
TST 263 - Testing for Path Traversal (NEW Duration: 15 minutes).....	27
TST 264 - Testing for Download of Code without integrity Check (NEW Duration: 15 minutes).....	27
TST 265 - Testing for Incorrect Authorization (NEW Duration: 15 minutes).....	27
TST 266 - Testing for Inclusion of Functionality from Untrusted Control Sphere (NEW Duration: 15 minutes).....	27
TST 267 - Testing for Incorrect Permission Assignment for Critical Resource (NEW Duration: 15 minutes).....	27
TST 268 - Testing for Use of a Potentially Dangerous Function (NEW Duration: 15 minutes).....	27
TST 269 - Testing for Use of a Broken or Risky Cryptographic Algorithm (NEW Duration: 15 minutes).....	28
TST 270 - Testing for Incorrect Calculation of Buffer Size (NEW Duration: 15 minutes).....	28
TST 271 - Testing for Improper Restriction of Excessive Authentication Attempts (NEW Duration: 15 minutes).....	28
TST 272 - Testing for Open Redirect (NEW Duration: 15 minutes).....	28
TST 273 - Testing for Uncontrolled Format String (NEW Duration: 15 minutes).....	28
TST 274 - Testing for Integer Overflow or Wraparound (NEW Duration: 15 minutes).....	29
TST 275 - Testing for Use of a One-Way Hash without a Salt (NEW Duration: 15 minutes).....	29

Security Essentials

ENG 110 - Essential Account Management Security (Duration: 15 minutes).....	30
ENG 111 - Essential Session Management Security (Duration: 15 minutes).....	30
ENG 112 - Essential Access Control for Mobile Devices (Duration: 15 minutes).....	30
ENG 113 - Essential Secure Configuration Management (Duration: 15 minutes).....	30
ENG 114 - Essential Risk Assessment (Duration: 15 minutes).....	30
ENG 115 - Essential System and Information Integrity (Duration: 15 minutes).....	30
ENG 116 - Essential Security Planning Policy and Procedures (Duration: 15 minutes).....	30
ENG 117 - Essential Information Security Program Planning (Duration: 15 minutes).....	31
ENG 118 - Essential Incident Response (Duration: 15 minutes).....	31
ENG 119 - Essential Security Audit and Accountability (Duration: 15 minutes).....	31
ENG 120 - Essential Security Assessment and Authorization (Duration: 15 minutes).....	31
ENG 121 - Essential Identification and Authentication (Duration: 15 minutes).....	31
ENG 122 - Essential Physical and Environmental Protection (Duration: 15 minutes).....	31
ENG 123 - Essential Security Engineering Principles (Duration: 15 minutes).....	32
ENG 124 - Essential Application Protection (Duration: 15 minutes).....	32
ENG 125 - Essential Data Protection (Duration: 15 minutes).....	32
ENG 126 - Essential Security Maintenance Policies (Duration: 15 minutes).....	32
ENG 127 - Essential Media Protection (Duration: 15 minutes).....	32

AWA 007**Information Privacy and Security Awareness for Executives**

Duration: 45 minutes

This course provides decision-makers and managers with a concise summary essential ISPA requirements. Content is aligned with the topics contained in our standard ISPA courses, ensuring managers and staff are focused on the same objectives.

AWA 008**Information Privacy - Classifying Data**

Duration: 15 minutes

This introductory course is designed for general staff in roles such as human resources, legal, marketing, finance, sales, operations and customer service. This course equips employees to recognize the importance of understanding what constitutes private data.

AWA 009**Information Privacy - Protecting Data**

Duration: 20 minutes

This introductory course is designed for general staff in roles such as human resources, legal, marketing, finance, sales, operations and customer service. This course equips employees to recognize the importance of understanding what constitutes private data and how to behave in a proactive manner to protect this information in their everyday work

AWA 010**Email Security**

Duration: 10 minutes

This security awareness course is intended to teach students how to recognize malicious email before it can become a threat, how to properly handle email, and best practices around how and when to use email to send specific types of information. Through participating in this courses, students will be able to define Personally Identifiable Information (PII), understand the impact of sending sensitive information over an insecure medium, and identify information that should not be sent by email.

AWA 012**Malware Awareness**

Duration: 10 minutes

This security awareness course is intended to teach students how to identify and define types of malware. Through participating in this course, students will be able to recognize evidence of active infection and understand what the proper actions are to prevent such attacks.

AWA 013**Mobile Security**

Duration: 15 minutes

This security awareness course is intended to give students a look at mobile device security. Through participating in this course, students will be able to list the characteristics of mobile device platforms and identify the role device ownership plays as a basis for understanding application risk.

AWA 014**Password Security**

Duration: 10 minutes

This security awareness course is intended to teach students how to create and remember strong passwords, therefore eliminating the need to use insecure practices. Through participating in this course, students will learn how to recognize the risks surrounding password security, identify safeguards used to protect passwords, and summarize techniques used by attackers to obtain passwords.

AWA 015**PCI Compliance**

Duration: 15 minutes

This security awareness course is intended to teach students to follow the PCI Security Standards in order to understand how to identify different types of sensitive data and handle it properly. Through participating in this course, students will be able to recognize appropriate protection mechanisms for cardholder data and acknowledge how the PCI DSS helps minimize risk to cardholder data.

AWA 016**Phishing Awareness**

Duration: 10 minutes

This security awareness course is intended to teach students how to recognize malicious email before it can become a threat. Through participating in this course, students will be able to understand the various ways in which attackers try to trick and entice users to trigger malicious events through email, as well as best practices to properly handle and avoid phishing attacks.

AWA 017**Physical Security**

Duration: 10 minutes

This course is intended to teach students accepted practices for minimizing breaches and give them the ability to identify different types of data that may be exposed via hardware theft. Through participating in this course, students will be able to understand what physical security is and why it is everyone's responsibility, identify common physical security attacks, and identify physical security best practices.

AWA 018**Social Engineering Awareness**

Duration: 15 minutes

This security awareness course is intended to teach students how to identify the many forms of social engineering and its potential impacts. Through participating in this course, students will be able to identify techniques used by social engineers and understand how to establish validity of requests in order to perform daily business functions in light of potential threats.

AWA 019**Travel Security**

Duration: 15 minutes

This security awareness course is intended to introduce students to the risks associated with transporting sensitive data. Through participating in this course, students will be able to recognize threats that may be present while traveling, identify the risks certain locations may harbor, and understand the defenses that you may employ while traveling.

AWA 101

Fundamentals of Application Security

Duration: 60 minutes

This course introduces the fundamentals of application security. It discusses the main drivers for application security, fundamental concepts of application security risk management, the anatomy of an application attack, some common attacks, the concept of input validation as a primary risk mitigation technique, and key security principles and best practices for developing secure applications.

AWA 102

Secure Software Concepts

NEW Duration: 30 minutes

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. When you have completed this course, you will be able to describe the current threat landscape and identify several common security vulnerabilities. You will also be able to list several resources for evaluating and mitigating the most common application security risks. You will be able to identify security-related tasks for each stage in a secure software development lifecycle, and list resources for implementing a security strategy based on your organization's actual risk profile, and leveraging other organization's experiences with secure development practices. Finally, you will be able to describe how to apply several security best practices to harden your security stance.

COD 101

Fundamentals of Secure Development

Duration: 60 minutes

This course introduces you to the need for secure software development, as well as the models, standards, and guidelines that you can use to understand security issues and improve the security posture of your applications. It also describes key application security principles and secure coding principles, and explains how to integrate secure development practices into the software development lifecycle.

COD 110

Fundamentals of Secure Mobile Development

Duration: 60 minutes

This course introduces developers to the common risks associated with Mobile applications including 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. The student is then given an overview of the Mobile application development best practices to reduce these risks including 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. Included is a discussion of threat modeling mobile applications. With knowledge checks throughout, the student who completes this course will have an understanding of mobile environment threats and risks, and the programming principles to use to address them.

COD 141

Fundamentals of Secure Database Development

Duration: 110 minutes

In practice, the database represents the goal of many attackers, as this is where the information of value is maintained. However, 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 is platform and technology agnostic, and will provide software architects and developers with an understanding of database development best practices.

COD 152**Fundamentals of Secure Cloud Development**

Duration: 30 minutes

This course introduces developers to the common risks associated with Cloud applications, including the security features of the different series models (IaaS, PaaS, and SaaS), how to identify and mitigate the most common vulnerabilities, the unique security challenges of "Big Data", and how to apply the Microsoft SDL to cloud applications. Threat coverage includes unauthorized account access, insecure APIs, shared technology, data leakage, and account hijacking, as well the importance of complying with regulatory requirements.

COD 153**Fundamentals of Secure AJAX Code**

Duration: 35 minutes

This course introduces security issues and challenges specific to AJAX applications. It provides an overview of AJAX technology, and presents common AJAX application vulnerabilities and attack vectors. Upon completion of this class, participants will be able to identify the differences between regular and AJAX applications, common AJAX vulnerabilities that attackers tend to exploit, and major threats to AJAX applications from cross-site scripting, cross-site request forgery, and injection attacks.

COD 160**Fundamentals of Secure Embedded Software Development**

Duration: 90 minutes

In this course, you will learn about security issues inherent to embedded device architecture. You will also learn about techniques to identify system security and performance requirements, develop appropriate security architecture, select the correct mitigations, and develop policies that can ensure the secure operation of your system.

COD 170**Identifying Threats to Mainframe COBOL Applications and Data**

Duration: 20 minutes

This 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 200**Creating Secure C Code Series**

Duration: 30 minutes

This series provides C developers with the knowledge and skills required to secure communications with Transport Layer Security (TLS) and to implement run-time protections with technologies such as stack security cookies, Address Space Layout Randomization (ASLR), and No-eXecute.

COD 201**Secure C Encrypted Network Communications**

Duration: 15 minutes

In this course, you will learn about secure communications using Transport Layer Security (TLS), and best practices for implementing these with your C and C++ applications. After completing this course, you will be able to identify the basic principles of TLS, identify libraries and interfaces for implementing the TLS protocol, identify TLS security considerations, and identify alternatives to TLS.

COD 202**Secure C Run-Time Protection**

Duration: 15 minutes

This course discusses common run-time protection technologies that you can use to protect your application from attack. After completing this course, you will be able to identify run-time protection technologies, such as stack security cookies, Address Space Layout Randomization, and No-eXecute. You will be also able to identify their limitations, and how to apply them to your applications.

COD 205**Creating Secure C++ Code Series**

Duration: 55 minutes

This series provides C++ developers with the knowledge and skills required to mitigate memory corruption vulnerabilities, protect data in transit using strong TLS ciphers, and to protect data using cryptographic best practices

COD 206**Creating Secure C++ Code**

Duration: 15 minutes

This course highlights some of the most useful security features for avoiding memory corruption vulnerabilities in C++, including:

- ¥ Using standard containers and their built-in functions to avoid direct memory operations
 - ¥ Using bounds-checking functions, especially for string manipulation, to avoid buffer overflows
 - ¥ Using smart pointers to avoid memory leaks associated with managing raw pointers
 - ¥ Using standard concurrency features to help reduce the risk of introducing race conditions
 - ¥ Using object-oriented programming features to define and manipulate data in terms of objects, thus avoiding direct memory operations that may lead to memory corruption
 - ¥ Using range-based loops to avoid off-by-one indexing errors
- Using native regular expressions to validate untrusted text input and avoid the risk of introducing vulnerabilities through third-party libraries.
-

COD 207**Communication Security in C++**

Duration: 15 minutes

This course discusses how to protect data in transit using encryption libraries and strong TLS ciphers. It also reviews important issues about public key certificates including signing and verifying them. After completing this course, you will be able to identify well-trusted encryption libraries and strong TLS cipher suites to protect data in transit, and explain how to protect and verify the integrity of public key certificates

COD 307**Protecting Data in C++**

NEW Duration: 25 minutes

This course discusses cryptography and related issues for COD 307 - Protecting Data in C++. After completing this course, you will be able to generate strong encryption keys and identify related symmetric cryptography issues, such as pseudo random number generators (PRNGs), key derivation algorithms, and initialization vectors. Additionally, you will be able to select an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode, and identify common libraries that support symmetric cryptography. You will also be able to identify key concepts of public key cryptography, explain how public and private key pairs work together both to encrypt and decrypt data for secure transfer and to create and verify digital signatures, and implement best practices to mitigate memory exposure vulnerabilities.

COD 215**Creating Secure Code .NET Framework Foundations Series**

NEW Duration: 75 minutes

English

This series provides you with secure coding techniques and best practices that will enable you to avoid common security flaws and ultimately build secure applications in .NET.

COD 216**Leveraging .NET Framework Code Access Security (CAS)**

NEW Duration: 30 minutes

English

This course provides you with the necessary information to help you understand the foundation of .NET, the CLR's native security infrastructure (Code Access Security), and the ASP.NET security infrastructure.

COD 217**Mitigating .NET Security Threats**

COMING SOON Duration: 45 minutes

English

This course provides you with secure coding techniques and best practices that will enable you to avoid common security flaws and ultimately build secure applications in .NET. Additionally, the course discusses secure error handling and secure logging in the context of preventing information disclosure and other vulnerabilities.

COD 219**Creating Secure Code - SAP ABAP Foundations**

Duration: 90 minutes

This course presents best practices and techniques for secure SAP application development using Java and ABAP. It discusses basic application security principles, input validation in SAP applications, common application security vulnerabilities and mitigations, protecting data using encryption, and conducting security code analysis and code reviews.

COD 222**PCI DSS v3.2 Best Practices for Developers**

Duration: 60 minutes

The Payment Card Industry Data Security Standard (PCI-DSS) Version 3.2 provides minimum requirements for addressing the security of software systems handling credit card information. Addressing the requirements during the design and build stages of the development lifecycle improves application security and simplifies compliance. This course will provide software developers with an in-depth understanding of application security issues within the PCI-DSS Version 3.2 and best practices for addressing each requirement.

COD 224**IoT Specialization Series**

Duration: 60 minutes

In this series, you will learn about the importance of integrating security into each stage of your IoT SDLC.

COD 225

Insecure IoT Web Interfaces

Duration: 10 minutes

In this course, you will learn how to identify common threats to IoT web interfaces and apply best practices to mitigate these threats.

COD 226

Insecure IoT Authentication and Authorization

Duration: 10 minutes

In this course, you will learn about how to implement secure authentication and authorization for Internet of Things (IoT) devices.

COD 227

Insecure IoT Network Services

Duration: 10 minutes

In this course, you will learn about the vulnerabilities of Insecure Network Services within the context of the Internet of Things (IoT) devices, and best practices to protect network services on IoT devices.

COD 228

Insecure IoT Communications

Duration: 10 minutes

In this course, you will learn about the risks of insecure communications.

COD 229

Insecure IoT Mobile Interface

Duration: 10 minutes

In this course, you will learn about best practices for protecting mobile applications used for IoT solutions

COD 230

Insecure IoT Firmware

Duration: 10 minutes

In this course, you will learn how to securely distribute updates that fix known vulnerabilities in software or firmware for your Internet of Things devices.

COD 233

OWASP Mobile Series

Duration: 80

In this series, you will learn about the importance of integrating security into each stage of your Mobile App Development SDLC.

COD 234

Mobile Threats and Mitigations

Duration: 20 minutes

In this course, you will learn about best practices for identifying and mitigating the most common threats to mobile applications and their data.

COD 235

Defending Mobile Data with Cryptography

Duration: 20 minutes

In this course, you will learn about best practices for implementing strong cryptography to protect mobile applications and their data.

COD 236

Mobile App Authentication and Authorization

Duration: 20 minutes

In this course, you will learn how to integrate secure authentication and authorization into your mobile application.

COD 237

Defending Mobile App Code

Duration: 20 minutes

In this course, you will learn about best practices for defending your mobile application's code from attacks.

COD 241

Creating Secure Oracle Database Applications

NEW Duration: 45 minutes

This course introduces database application developers to key industry best practices for data security, such as secure query construction and secure communication and storage. After completing this course, you will be able to describe how to write stored procedures securely. You will also be able to explain how to secure data stored in the database as well as data in transit using Oracle Database features.

COD 242

Creating Secure SQL Server and Azure SQL Database Applications

Duration: 40 minutes

In this course, you will learn how to protect sensitive data and while ensuring the integrity of applications running on the Microsoft SQL Server Engine and Azure SQL Database.

COD 251

Creating Secure AJAX Code - ASP.NET Foundations

Duration: 90 minutes

This course introduces secure ASP.NET coding principles for AJAX applications. It provides an overview of best practices to mitigate common vulnerabilities and protect against common attack vectors. Upon completion of this class, participants will be able to identify the threats to AJAX applications from cross-site scripting, cross-site request forgery, and injection attacks, and ways to implement countermeasures against these attacks by protecting client resources, validating input, protecting web services requests, preventing request forgeries, and securing data access.

COD 252**Creating Secure AJAX Code - Java Foundations**

Duration: 35 minutes

This course introduces secure Java coding principles for AJAX applications. It provides an overview of best practices to mitigate common vulnerabilities and protect against common attack vectors. Upon completion of this class, participants will be able to identify the most common threats to AJAX applications from cross-site scripting, cross-site request forgery, and injection attacks, and ways to implement countermeasures against attacks by protecting client resources, validating input, restricting access to Ajax services, and preventing request forgeries.

COD 253**Creating Secure AWS Cloud Applications**

Duration: 60 minutes

This course examines the security vulnerabilities, threats, and mitigations for AWS cloud computing services. It includes coverage of dedicated AWS security features, such as Key Management Service (KMS), Hardware Security Module (HSM), Identity and Access Management (IAM), and CloudWatch. In addition, it discusses 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**

Duration: 90 minutes

This course examines the security vulnerabilities, threats, and mitigations for Azure cloud computing services. After completing this course, you will be able to identify the most common security threats to cloud based applications and best practices to protect against these threats. You will also be able to identify key Azure security platforms and services that you can use to improve the security of your applications.

COD 255**Creating Secure Code - Web API Foundations**

Duration: 120 minutes

This course introduces the fundamentals of secure web services development. It describes common web services threats that might put your application at risk, and reviews best practices that you should incorporate to mitigate the risks from web services attacks. After completing this course, you will be able to describe various web services threats, explain the cause and impact of web services attacks, and implement secure development best practices to help protect web services.

COD 256**Creating Secure Code - Ruby on Rail Foundations**

Duration: 90 minutes

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.

COD 257**Creating Secure Python Web Applications**

Duration: 45 minutes

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.

COD 259**Node.js Threats and Vulnerabilities**

NEW Duration: 30 minutes

This course discusses system configuration, injection attacks, session management, package management, and the AngularJS framework, all within the context of Node.js security.

COD 260**Secure Scripting Series**

Duration: Unknown

In this series, you will learn about how to identify security threats to scripts and how to mitigate those threats by implementing access controls and following secure scripting best practices.

COD 261**Threats to Scripts**

Duration: 30 minutes

In this course, you will learn about the impact of incorrect script development or lax security measures. You will also learn about the most common scripting vulnerabilities, including cached secrets, a variety of injection vulnerabilities, weaknesses related to permissions and privileges, and the threat of resource exhaustion.

COD 262**Fundamentals of Secure Scripting**

Duration: 30 minutes

In this course, you will learn about how shell scripting languages compare with more modern interpreted languages, several information security principles including least privilege and defense in depth, the importance of data validation, and operating system portability issues.

COD 263**Secure Scripting with Perl, Python, Bash and Ruby**

Duration: 30 minutes

In this course, you will learn about the importance of error and exception handling in shell scripts and interpreted languages, common syntax pitfalls, and how to prevent or mitigate several common vulnerabilities.

COD 264**Protecting Sensitive Data while Scripting**

Duration: 30 minutes

In this course, you will learn about how to use filesystem operations safely to protect files, techniques for system hardening, cryptography basics, and the importance of up-to-date communication security techniques.

COD 270**Creating Secure COBOL and Mainframe Applications**

Duration: 25 minutes

This course covers countermeasures for security vulnerabilities on the mainframe, such as input validation, parameterized APIs, strong cryptography, and being aware of memory management issues

COD 280**Creating Secure Java Series**

Duration: 70 minutes

This series provides Java developers with the knowledge and skills required to implement the Java Security Model, JAAS, and to protect data using cryptographic best practices.

COD 281**Java Security Model**

Duration: 20 minutes

This course introduces you to Java's policy-driven security model. Key topics include the Java security model, the Java security manager, security policies, and security policy files. After completing this course, you will be able to identify the components of the Java security model and the functionality of the Java security manager and access controller. You will also be able to identify the components of Java security policies as well as describe the function of Java security policy files.

COD 282**Java Authentication and Authorization (JAAS)**

Duration: 20 minutes

This course discusses the Java authentication and authorization service, or JAAS. JAAS is a Java implementation of the standard pluggable authentication module, or PAM, framework. JAAS provides a framework that developers can use to require users to log in and to define precisely which actions users can perform.

After completing this course, you will be able to identify the components of the JAAS framework, and identify how to use JAAS to control user authentication and authorization in your Java application.

COD 283**Java Cryptography**

Duration: 30 minutes

This course discusses cryptography and related issues in Java. After completing this course, you will be able to generate secure encryption keys and identify related issues such as pseudo random number generators, key derivation functions, and initialization vectors. You will also be able to select an appropriate symmetric encryption algorithm, cipher mode, and authenticated encryption mode. You will also be able to identify key concepts of public key cryptography, explain how public and private key pairs work together to encrypt and decrypt data for secure transfer and to create and verify digital signatures, and use the Java keytool command-line utility for creating and managing keys and keystores.

COD 300

Protecting C Code Series

Duration: 95 minutes

This series provides C developers with the knowledge and skills required to mitigate buffer overflow conditions, implement secure memory management best practices, and protect applications and data from attacks.

COD 301

Secure C Buffer Overflow Mitigations

Duration: 45 minutes

The C and C++ languages cover a wide range of systems spanning several decades of development. Although all programming languages are susceptible to security vulnerabilities, C and C++ are particularly prone to them due to the low-level nature of the language. In this course, you will learn how to prevent the most serious vulnerabilities in your C and C++ applications. After completing this course, you will be able to mitigate buffer overflows, understand and prevent several additional types of memory management vulnerabilities, protect data in memory, prevent format string vulnerabilities, understand integer overflows, mitigate race conditions, and avoid the most common types of Injection vulnerabilities.

COD 302

Secure C Memory Management

Duration: 30 minutes

After completing this course, you will be able to identify the key concepts of dynamic memory management, identify common mistakes that lead to memory corruption and vulnerabilities, and implement best practices to mitigate memory management vulnerabilities.

COD 303

Common C Vulnerabilities and Attacks

Duration: 20 minutes

In this course you will review common C application vulnerabilities, how they manifest in code, and 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 format string attacks, integer overflows, race conditions, canonicalization issues, command injection, and SQL Injection.

COD 311

Creating Secure Code ASP.NET MVC Applications

Duration: 90 minutes

In this course, you will learn about ASP.NET MVC and Web API code security issues that affect MVC and Web API applications. You'll learn methods to protect your application from attacks against MVC's model-binding behavior, as well as methods to protect your application from cross-site scripting, cross-site request forgery, and malicious URL redirects. You will also study the Web API pipeline and how to implement authentication and authorization in Web API applications.

COD 315

Creating Secure PHP Code

Duration: 120 minutes

This course teaches PHP programmers the security principles they need to know to build secure PHP applications. This class teaches programming principles for security in PHP such as proper session management, error handling, authentication, authorization, data storage, use of encryption and defensive programming as well as avoiding and mitigating vulnerabilities such as SQL Injections, Cross-Site Scripting (XSS), File Inclusion, Command Injection, Cross Site Request Forgery (CSRF) and Null Byte attacks. With interactive knowledge checks in each of the modules, after completing the course, the student will be able to program securely and defensively in PHP.

COD 316**Creating Secure iOS Code in Objective C**

COMING SOON Duration: 30 minutes

This course discusses techniques for creating secure iOS applications. It covers several common vulnerabilities, such as exposure of authentication credentials, sensitive data, and other secrets; custom URL scheme abuse; and XML eXternal Entity (XXE) Injection. It also describes techniques for mitigating these vulnerabilities. After you have completed this course, you will be able to protect data at rest with the Data Protection and Common Crypto APIs, mitigate sensitive data exposure in background snapshots, prevent custom URL scheme abuse, and mitigate XXE Injection.

COD 317**Creating Secure iOS Code in Swift**

Duration: 90 minutes

In this course you will learn how to identify the most common iOS application security vulnerabilities, including Insecure Data Storage, Side Channel Data Leakage, Client Side Injection, Custom URL Scheme Abuse, Stack Smashing and Self-Signed Certificates. You will learn how to mitigate these threats by leveraging iOS and Swift security services while also implementing secure coding best practices, including Secure Memory Management, Automatic Reference Counting, Enabling Position Independent Executable, Secure Data Storage, Communicating Over HTTPS, App Transport Security, TLS Certificate Pinning, Asymmetric Encryption, Parameterized SQL Queries, Validating Path Location Input and Implementing Apple Pay.

COD 318**Creating Secure Android Code in Java**

Duration: 90 minutes

In this course you will learn how to identify and mitigate the most common Android application security vulnerabilities and attack vectors, including: Weak Server Side Controls, Threats to Data, SQL Injection, Cross-Site Scripting (XSS), Session Hijacking, Threats to User Privacy and Confidentiality, Native Code Attacks, and Missing Data Encryption. Mitigation and best-practices include the Android software stack, the Android security model, access control methods, sandboxing, interprocess communications and implementing the security features of open-source developer tools.

COD 320**Protecting C# Series**

NEW Duration: 90 minutes

This series describes methods that will produce secure C# applications. It presents the common security vulnerabilities "Canonicalization Issues" and "Integer Overflows", and the unique features of C# and the .NET Framework that can be used to mitigate them.

COD 321**Protecting C# from Integer Overflows and Canonicalization Issues**

NEW Duration: 30 minutes

This course describes methods that will produce secure C# applications. It presents the common security vulnerabilities "Canonicalization Issues" and "Integer Overflows", and the unique features of C# and the .NET Framework that can be used to mitigate them.

COD 322**Protecting C# from SQL and XML Injection**

NEW Duration: 35 minutes

This course presents some of the most pervasive security vulnerabilities, "SQL Injection" and "XML Injection", and the features of the .NET Framework that can be used to mitigate them. When you have completed this course, you will be able to explain where and when SQL injection and XML injection are likely to occur, identify common pitfalls when defending against these vulnerabilities, and identify best practices for mitigating these vulnerabilities.

COD 323**Protecting Data in C#**

NEW Duration: 25 minutes

This course describes protecting data both in transit and at rest in C# applications using strong cryptography. Included examples show how sensitive data can be protected in memory with the SecureString and ProtectedMemory classes. The course also describes common cryptographic pitfalls you should avoid, and finally discusses how to protect data in transit, preferably with Transport Layer Security (TLS).

COD 352**Creating Secure jQuery Code**

Duration: 90 minutes

In this course, you will learn about common client-side vulnerabilities and threats to jQuery applications, and techniques for mitigating these vulnerabilities and threats. You will also learn about how to implement new HTML5 security features to secure JQuery applications, and best practices to secure local storage and implement transport layer security. After completing this course, you will be able to describe the threats that can impact your jQuery code and describe the countermeasures to address these threats.

COD 360**Creating Secure HTML5 Code Series**

NEW Duration: 75 minutes

English

This series provides in depth coverage on how to identify and mitigate the most dangerous threats to HTML5 applications, including exposure of sensitive data and insecure communications. In addition it describes how to leverage important HTML5 security features.

COD 361**HTML5 Security Threats**

NEW Duration: 15 minutes

English

In this course, you will learn about security risks introduced by HTML5. You will also learn about threats, including cross-site scripting, cross-site request forgery, clickjacking, and threats to user privacy, as well as techniques for mitigating these threats.

COD 362**HTML5 Built-In Security Features**

NEW Duration: 20 minutes

English

In this course, you will learn about important HTML5 security features, including Same-Origin Policy (SOP), Content Security Policy (CSP), Cross-Origin Resource Sharing (CORS), and IFrame Sandboxing, including examples and best practices.

COD 363**Securing HTML5 Data**

NEW Duration: 20 minutes

English

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-Sent Events, and best practices for the Web Workers, History, Geolocation, and Drag and Drop APIs.

COD 364

Securing HTML5 Connectivity

NEW Duration: 20 minutes
English

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

COD 379

Protecting Java Code Series

NEW Duration: 65 minutes

This series provides Java developers with the knowledge and skills required to mitigate the most common application security vulnerabilities, including SQLi, XSS, and Information Disclosure.

COD 380

Protecting Java Code: SQLi and Integer Overflows

NEW Duration: 10 minutes

This course describes ways to remediate common application security vulnerabilities in your Java application. After completing this course, you will be able to mitigate risk from SQL injection and integer overflows.

COD 381

Protecting Java Code: Canonicalization, Information Disclosure and TOCTOU

NEW Duration: 25 minutes

This course describes ways to remediate common application security vulnerabilities in your Java application. After completing this course, you will be able to mitigate risk from canonicalization issues, information disclosure, and race conditions.

COD 382

Protecting Data in Java

NEW Duration: 30 minutes

After completing this course, you will be able to mitigate risk from SQL injection and integer overflows.

DES 101

Fundamentals of Secure Architecture

Duration: 60 minutes

In the past, software applications were created with little thought to the importance of security. In recent times, businesses have become more rigorous about how they buy software. When looking at applications and solutions, companies don't just look at features, functionality, and ease of use. They focus on the total cost of ownership (TCO) of what they purchase. Security is a large and visible part of the TCO equation. In this course, students will examine the state of the industry from a security perspective. They will then look at some of the biggest security disasters in software design and what lessons can be learned from them. Finally, participants will understand and use confidentiality, integrity, and availability as the three main tenets of information security. Upon completion of this course, participants will understand the state of the software industry with respect to security by learning from past software security errors and will avoid repeating those mistakes, and they will understand and use confidentiality, integrity, and availability (CIA) as the three main tenets of information security.

DES 201

Fundamentals of Cryptography Series

NEW Duration: 120 minutes

English

In this series, you will learn basic concepts of cryptography and common ways that it is applied, from the perspective of application development. You will learn the importance of randomness; the roles of encoding, encryption, and hashing; the concepts of symmetric and asymmetric encryption; the purpose of cryptographic keys; and the roles of message authentication codes (MACs) and digital signatures. In addition, you'll be introduced to key management, digital certificates, and the public key infrastructure (PKI).

DES 202

Cryptographic Suite Services: Encoding, Encrypting and Hashing

NEW Duration: 45 minutes

English

This course presents an overview of the fundamental services provided by cryptographic suites, namely encoding, encrypting and hashing. After completing this course, you will be able to explain encoding and decoding, encryption and decryption, the difference between encoding and encryption, and explain hashing. You will also be able to identify the appropriate applications of these services. This course coverage aligns with the National Initiative for Cybersecurity Education (NICE) requirement K0018: Knowledge of encryption algorithms.

DES 203

Cryptographic Components: Randomness, Algorithms, and Key Management

NEW Duration: 15 minutes

English

This course introduces the common components of cryptographic systems including random number generation, algorithms to perform cryptographic manipulation of information, cryptographic keys, and a mechanism to manage and distribute cryptographic keys. This course coverage aligns with the National Initiative for Cybersecurity Education (NICE) requirements K0018: Knowledge of encryption algorithms, and K0019: Knowledge of cryptography and cryptographic key management concepts.

DES 204

The Role of Cryptography in Application Development

NEW Duration: 15 minutes

English

This course introduces cryptography and how cryptography can help secure applications and data. It also provides an overview of common uses of cryptography. After completing this course, you will be able to identify the various cryptographic technologies that are relevant to software solutions. You will also be able to identify several common data-in-motion cryptographic security applications, and identify several common data-at rest cryptographic security applications.

DES 205

Message Integrity Cryptographic Functions

NEW Duration: 45 minutes

English

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. This course coverage aligns with the National Initiative for Cybersecurity Education (NICE) requirements K0018: Knowledge of encryption algorithms, and K0019: Knowledge of cryptography and cryptographic key management concepts.

DES 212

Architecture Risk Analysis and Remediation

Duration: 60 minutes

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.

DES 213

Secure Enterprise Infrastructure Series

Duration: 120 minutes

In this series, you will learn about the importance of designing and implementing secure access controls across the enterprise infrastructure. You will also learn about the techniques used to identify system security and performance requirements, develop appropriate security architecture, select the correct mitigations, and develop policies that can ensure the secure operation of your systems.

DES 214

Securing Network Access

Duration: 30 minutes

In this course, you will learn about how Network Access Control can be used to secure systems on a network, including how to integrate strong authentication, and how to enforce policies, and how using a centralized monitoring system to log system access and system use can be useful in recognizing and containing attacks.

DES 215

Securing Operating System Access

Duration: 30 minutes

This course equips employees to recognize the importance of understanding what constitutes private data and how to behave in a proactive manner to protect this information in their everyday work. In this course, you will learn about common operating system threats and how to best mitigate those threats. It also describes the benefits of multi-factor authentication, strong password management, and user account controls, and explains the benefits and risks associated with secure ID tokens, biometrics, and single sign-on (SSO).

DES 216

Securing Cloud Instances

Duration: 30 minutes

In this course, you will learn about the top threats to Cloud resources and how to mitigate them using application security best practices.

DES 217

Application, Technical and Physical Access Controls

Duration: 30 minutes

In this course, you will learn about the risks associated with data breaches and how to implement strong access controls and security policies that protect applications, systems and sensitive data.

DES 221

OWASP 2017 Series

Duration: 120 minutes

The primary objective of this series of courses, and of the OWASP Top 10, is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses.

DES 222

Applying OWASP 2017: Mitigating Injection

Duration: 12 minutes

In this course, you will learn how to mitigate the risks associated with broken authentication.

DES 223

Applying OWASP 2017: Mitigating Broken Authentication

Duration: 12 minutes

In this course, you will learn how to mitigate the risks associated with broken authentication.

DES 224

Applying OWASP 2017: Mitigating Sensitive Data Exposure

Duration: 12 minutes

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

DES 225

Applying OWASP 2017: Mitigating XML External Entities (XXE)

Duration: 12 minutes

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

DES 226

Applying OWASP 2017: Mitigating Broken Access Control

Duration: 12 minutes

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

DES 227

Applying OWASP 2017: Mitigating Security Misconfiguration

Duration: 12 minutes

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

DES 228

Applying OWASP 2017: Mitigating Cross Site Scripting (XSS)

Duration: 12 minutes

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

DES 229

Applying OWASP 2017: Mitigating Insecure Deserialization

Duration: 12 minutes

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

DES 230

Applying OWASP 2017: Mitigating Use of Components with Known Vulnerabilities

Duration: 12 minutes

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

DES 231

Applying OWASP 2017: Mitigating Insufficient Logging & Monitoring Vulnerabilities

Duration: 12 minutes

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

DES 260

Fundamentals of IoT Architecture and Design

NEW Duration: 30 minutes

This course focuses on topics in architecting and designing a secure Internet of Things (IoT) system, with emphasis on an embedded IoT device and its relationship with the cloud. Topics discussed range from what should be reviewed and defined in the requirements phase to authorization considerations within the IoT device and cloud.

DES 311

Creating Secure Application Architecture

Duration: 120 minutes

This course covers a set of key security principles that students can use to improve the security of application architecture and design. Principles of this course 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, and reducing the risk in error code paths.

DES 352

Creating Secure Over the Air (OTA) Automotive System Updates

Duration: 90 minutes

In this course, you will learn about the secure design considerations for over-the-air (OTA) updates for automotive systems. After completing this course, you will be able to identify the benefits and risks of OTA automotive system updates, understand the importance of public key cryptography to the security of these updates, and identify secure design considerations for development, delivery, and installation of OTA automotive system updates.

ENG 190

Implementing the MS SDL Process Into your SDLC

NEW Duration: 97 minutes

English

This series introduces the fundamentals of the Microsoft Security Development Lifecycle (SDL) process and covers the security requirements for each phase your SDLC. Agile SDL variation, the Security Development Lifecycle for Line-of-Business Applications (SDL-LOB), and the Microsoft SDL Threat Modeling tool.

ENG 191

Introduction to the Microsoft SDL

NEW Duration: 25 minutes

English

This course describes the main phases of the Microsoft Security Development Lifecycle (SDL) process, namely Requirements, Design, Implementation, Verification, and Release, with a focus on security throughout. After completing this course, you will be able to list the phases of the Microsoft SDL process, and describe the required and recommended tasks for each phase of the process

ENG 192

Implementing the Agile MS SDL

NEW Duration: 20 minutes

English

This course describes the Agile variation of the Microsoft Security Development Lifecycle (SDL) process. The standard MS SDL process follows the traditional incremental waterfall model, while Agile methodologies are more iterative. SDL-Agile maps critical security practices into every-sprint requirements, bucket or periodic requirements, and one-time requirements.

ENG 193

Implementing the MS SDL Optimization Model

NEW Duration: 12 minutes

English

This course introduces the Microsoft Security Development Lifecycle (SDL) Optimization Model and how to use it.

ENG 194

Implementing MS SDL Line of Business

NEW Duration: 20 minutes

English

This course describes the Microsoft Security Development Lifecycle for Line of Business (SDL-LOB), aimed at development of internal or business-facing applications. Important activities include security training, risk assessment, and the typical software lifecycle phases: Requirements, Design, Implementation, Verification, and Release.

ENG 195

Implementing the MS SDL Threat Modeling Tool

NEW Duration: 20 minutes

English

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, use of the tool aids teams with the creation of threat models and helps enumerate threats using STRIDE.

ENG 205

Fundamentals of Threat Modeling

Durations: 60 minutes

In this course, you will learn how to question-driven approach to threat modeling that can help you identify security design problems early in the application design process.

ENG 211

How to Create Application Security Design Requirements

Duration: 60 minutes

Security is an important component of an application's quality. To preserve the confidentiality, integrity, and availability of application data, software applications must be engineered with security in mind beginning with the design phase. 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 tools to understand, create and articulate security requirements as part of a software requirement documents. In this course, students will learn to apply the application security maturity (ASM) model to the development process, understand the security-engineering process, and describe the key security-engineering activities to integrate security in the development life cycle. Students will also be able to determine software security objectives, apply security design guidelines, and create threat models that identify threats, attacks, vulnerabilities, and countermeasures, in addition to learning to conduct security architecture and design reviews that help identify potential security problems, and minimize the application's attack surface.

ENG 311

Attack Surface Analysis & Reduction

Duration: 60 minutes

Attack surface analysis and reduction is an exercise in risk reduction. The attack surface of an application represents the number of entry points exposed to a potential attacker of the software. The larger the attack surface, the larger the set of methods that can be used by an adversary to attack. The smaller the attack surface, the smaller the chance of an attacker finding a vulnerability and the lower the risk of a high impact exploit in the system. This course provides an understanding of the goals and methodologies of attackers, identification of attack vectors, and how to minimize the attack surface of an application. In this course, students will learn to define the attack surface of an application, and how to reduce the risk to an application by minimizing the application's attack surface.

ENG 312

How to Perform a Security Code Review

Duration: 60 minutes

Application developers may use a variety of tools to identify flaws in their software. Many of these tools, however, cannot be deployed 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. Manual code reviews, in contrast, can begin at any time and require no specialized tools - only secure coding knowledge. Manual code reviews can also be laborious if every line of source code is reviewed. This course provides students with guidance on how to best organize code reviews, prioritize those code segments that will be reviewed, best practices for reviewing source code and maximize security resources.

TST 101

Fundamentals of Security Testing

Duration: 120 minutes

This course introduces security-testing concepts and processes that will help students analyze an application from a security perspective and to conduct effective security testing. The course focuses on the different categories of security vulnerabilities and the various testing approaches that target these classes of vulnerabilities. Several manual and automated testing techniques are presented which will help identify common security issues during testing and uncover security vulnerabilities.

TST 221

Testing for OWASP 2017 Series

NEW Duration: 114 minutes

The Open Web Application Security Project (OWASP) Top Ten is a listing of critical security flaws found in web applications. Organizations that address these flaws greatly reduce the risk of a web application being compromised, and testing for these flaws is a requirement of the Payment Card Industry Standards (PCI-DSS) as well as other regulatory bodies. This course explains how these flaws occur and provides testing strategies to identify the flaws in web applications.

TST 222

Testing for OWASP 2017: Injection

NEW Duration: 15 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A1:2017 family of injection security vulnerabilities identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against these vulnerabilities. In this course, you will learn how to test your application against injection, and you will learn how to protect your applications against injection.

TST 223

Testing for OWASP 2017: Broken Authentication

NEW Duration: 12 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A2:2017 security vulnerability, broken authentication, identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application against broken authentication, and you will learn how to protect your applications against broken authentication.

TST 224

Testing for OWASP 2017: Sensitive Data Exposure

NEW Duration: 12 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A3:2017 security vulnerability, sensitive data exposure, identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application against sensitive data exposure, and you will learn how to protect your applications against sensitive data exposure.

TST 225**Testing for OWASP 2017: XML External Entities**

NEW Duration: 10 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A4:2017 security vulnerability, XML external entities, identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application against XML external entities, and you will learn how to protect your applications against XML external entities.

TST 226**Testing for OWASP 2017: Broken Access Control**

NEW Duration: 10 minutes

The Open Web Application Security Project (OWASP) Top 10 lists the most serious and prevalent security vulnerabilities identified for Web applications. This course explains the second vulnerability identified in the OWASP Top 10, Broken Access Control, and the mitigations you can use to reduce the risk to your application. After completing this course, you will be able to determine if a Web application is vulnerable to Broken Access Control, and explain how to protect the application against this security.

TST 227**Testing for OWASP 2017: Security Misconfiguration**

NEW Duration: 10 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A6:2017 vulnerability, security misconfiguration, identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application for security misconfiguration, and you will learn how to protect your application against security misconfiguration.

TST 228**Testing for OWASP 2017: Cross Site Scripting**

NEW Duration: 15 minutes

The Open Web Application Security Project (OWASP) Top 10 lists the most serious and prevalent security vulnerabilities identified for Web applications. This course explains the seventh vulnerability identified in the OWASP Top 10, Cross-Site Scripting (XSS), and the mitigations you can use to reduce the risk to your application. After completing this course, you will be able to determine if a Web application is vulnerable to Cross-Site Scripting vulnerabilities, and explain how to protect the application.

TST 229**Testing for OWASP 2017: Insecure Deserialization**

NEW Duration: 10 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A8:2017 Insecure Deserialization vulnerability identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application for insecure deserialization and you will learn how to protect your application against insecure deserialization.

TST 230**Testing for OWASP 2017: Use of Components with Known Vulnerabilities**

NEW Duration: 10 minutes

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, identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application for using components with known vulnerabilities and you will learn how to protect your application against using components with known vulnerabilities.

TST 231**Testing for OWASP 2017: Insufficient Logging and Monitoring**

NEW Duration: 10 minutes

This course explains how testers and developers can determine if their web applications are vulnerable to the A10:2017 Insufficient Logging and Monitoring vulnerability identified by the Open Web Application Security Project (OWASP). It also explains how to protect web applications against this vulnerability. In this course, you will learn how to test your application for insufficient logging and monitoring, and you will learn how to protect your application against insufficient logging and monitoring.

TST 250**Testing for CWE SANS Top 25 Software Errors Series**

NEW

English

In this series, you will learn how to identify and mitigate each of the CWE's 25 Most Dangerous Software Errors. Coverage includes techniques for spotting common security issues through code review and testing. Secure coding best practices are included for each security defect, as well as descriptions of technology specific weaknesses. The course includes Knowledge Checks, Module Summaries, and information about additional online resources.

TST 251**Testing for SQL Injection**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection). Coverage includes techniques for spotting SQL Injection through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 252**Testing for OS Command Injection**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection). Coverage includes techniques for spotting OS Command Injection through code review testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 253**Testing for Classic Buffer Overflow**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-120: Buffer Copy without Checking Size of Input. Coverage includes techniques for spotting Classic Buffer Overflow through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 254**Testing for Cross-site Scripting**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), or XSS. Coverage includes techniques for spotting Cross-site Scripting through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 255**Testing for Missing Authentication for Critical Function**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-306: Missing Authentication for Critical Function. Coverage includes techniques for spotting the Missing Authentication vulnerability through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 256**Testing for Missing Authorization**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-862: Missing Authorization. Coverage includes techniques for spotting Missing Authorization through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 257**Testing for Use of Hard-Coded Credentials**

NEW Duration: 15 minutes

English

[1] In this course, you will learn how to identify and mitigate CWE-798: Use of Hard- coded Credentials. Coverage includes techniques for spotting Hard-coded credential weaknesses through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-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.

TST 258

Testing for Missing Encryption of Sensitive Data

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-311: Missing Encryption of Sensitive Data. Coverage includes techniques for spotting Missing Encryptions through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- specific weaknesses as appropriate.

TST 259

Testing for Unrestricted Upload of File with Dangerous Type

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-434: Unrestricted Upload of File with Dangerous Type. Coverage includes techniques for spotting Unrestricted Upload vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-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.

TST 260

Testing for Reliance on Untrusted Inputs in a Security Decision

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-807: Testing for Reliance on Untrusted Inputs in a Security Decision. Coverage includes techniques for spotting Reliance on Untrusted Inputs vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 261

Testing for Execution with Unnecessary Privileges

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-250: Testing for Execution with Unnecessary Privileges. Coverage includes techniques for spotting Execution with Unnecessary Privileges vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 262

Testing for Cross Site Request Forgery

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-352: Cross-site Request Forgery (CSRF). Coverage includes techniques for spotting CSRF vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 263**Testing for Path Traversal**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-22: Testing for Path Traversal. Coverage includes techniques for spotting Path Traversal weaknesses through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-specific weaknesses as appropriate.

TST 264**Testing for Download of Code without integrity Check**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-494: Testing for Download of Code without Integrity Check. Coverage includes techniques for spotting weaknesses through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-specific weaknesses as appropriate.

TST 265**Testing for Incorrect Authorization**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-863: Incorrect Authorization. Coverage includes techniques for spotting Incorrect Authorization vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-specific weaknesses as appropriate.

TST 266**Testing for Inclusion of Functionality from Untrusted Control Sphere**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-829: Inclusion of Functionality from Untrusted Control Sphere. Coverage includes techniques for spotting CWE-829 weaknesses through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-specific weaknesses as appropriate.

TST 267**Testing for Incorrect Permission Assignment for Critical Resource**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-732: Testing for Incorrect Permission Assignment for Critical Resource. Coverage includes techniques for spotting CWE-732 vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-specific weaknesses as appropriate.

TST 268**Testing for Use of a Potentially Dangerous Function**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-676: Testing for Use of a Potentially Dangerous Function. Coverage includes techniques for spotting CWE-676 vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform-specific weaknesses as appropriate.

TST 269**Testing for Use of a Broken or Risky Cryptographic Algorithm**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-327: Testing for Use of a Broken or Risky Cryptographic Algorithm. Coverage includes techniques for spotting CWE-327 vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- specific weaknesses as appropriate.

TST 270**Testing for Incorrect Calculation of Buffer Size**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-131: Testing for Incorrect Calculation of Buffer Size. Coverage includes techniques for spotting CWE-131 vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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. Upon completion of this course, you will be able to identify CWE-131 vulnerabilities, recognize its potential impact, apply coding best practices to avoid it, find CWE-131 vulnerabilities in your application's source code, and test your application to detect it.

TST 271**Testing for Improper Restriction of Excessive Authentication Attempts**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-307: Testing for Improper Restriction of Excessive Authentication Attempts. Coverage includes techniques for spotting CWE-307 vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- specific weaknesses as appropriate.

TST 272**Testing for Open Redirect**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-601: Open Redirect. Coverage includes techniques for spotting CWE-601 vulnerabilities through codereview and testing. Secure coding best practices are included, as well as descriptions of technology and platform- 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.

TST 273**Testing for Uncontrolled Format String**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-134: Testing for Uncontrolled Format String. Coverage includes techniques for spotting CWE-134 vulnerabilities through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- specific weaknesses as appropriate.

TST 274**Testing for Integer Overflow or Wraparound**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-190: Testing for Integer Overflow or Wraparound. Coverage includes techniques for spotting weaknesses through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- specific weaknesses as appropriate.

TST 275**Testing for Use of a One-Way Hash without a Salt**

NEW Duration: 15 minutes

English

In this course, you will learn how to identify and mitigate CWE-759: Testing for Use of a One-Way Hash without a Salt. Coverage includes techniques for spotting weaknesses through code review and testing. Secure coding best practices are included, as well as descriptions of technology and platform- specific weaknesses as appropriate.

ENG 110**Essential Account Management Security**

Duration: 15 minutes

This course provides essential guidance to information system managers, designers and program managers on implementing specific account management security controls at the hardware and software level to facilitate compliance with applicable regulatory requirements.

ENG 111**Essential Session Management Security**

Duration: 15 minutes

This course provides essential guidance to system designers and developers on implementing specific session management security controls at the software level to facilitate compliance with applicable regulatory requirements.

ENG 112**Essential Access Control for Mobile Devices**

Duration: 15 minutes

This course provides essential guidance to mobile system designers and developers on implementing technical controls at the software and device level to facilitate compliance with applicable regulatory requirements.

ENG 113**Essential Secure Configuration Management**

Duration: 15 minutes

This course provides essential guidance to program managers, system designers and developers responsible for the effective implementation of selected security controls and control enhancements to help ensure compliance with applicable regulatory requirements.

ENG 114**Essential Risk Assessment**

Duration: 15 minutes

This course provides essential guidance to individuals with information system, security, and/or risk management and oversight responsibilities that include defining the purpose, scope, roles, management commitment, and coordination among organizational entities to help ensure compliance with applicable regulatory requirements.

ENG 115**Essential System and Information Integrity**

Duration: 15 minutes

This course provides essential guidance to program managers, system designers and developers on identifying systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel.

ENG 116**Essential Security Planning Policy and Procedures**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing and disseminating an organization-wide security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

ENG 117**Essential Information Security Program Planning**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing and disseminating an organization-wide information security program plan to facilitate compliance with applicable regulatory requirements.

ENG 118**Essential Incident Response**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for implementing an incident response policy and associated controls to help ensure compliance with applicable regulatory requirements.

ENG 119**Essential Security Audit and Accountability**

Duration: 15 minutes

This course provides essential guidance to information system owners, system administrators, and information system security officers developing procedures to facilitate the implementation of the audit and accountability policy and controls to facilitate compliance with applicable regulatory requirements.

ENG 120**Essential Security Assessment and Authorization**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing and implementing personnel security policy and associated personnel security controls to help ensure compliance with applicable regulatory requirements.

ENG 121**Essential Identification and Authentication**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing identification and authentication policy and controls to help ensure compliance with applicable regulatory requirements.

ENG 122**Essential Physical and Environmental Protection**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing physical and environmental protection policy and associated physical and environmental protection controls to help ensure compliance with applicable regulatory requirements.

ENG 123**Essential Security Engineering Principles**

Duration: 15 minutes

This course provides essential guidance to program managers, system designers, developers, information security engineers and systems integrators responsible for applying security-engineering principles to new development information systems or systems undergoing major upgrades.

ENG 124**Essential Application Protection**

Duration: 15 minutes

This course provides essential guidance to system designers and developers on implementing specific application security controls at the software level to facilitate compliance with applicable regulatory requirements.

ENG 125**Essential Data Protection**

Duration: 15 minutes

This course provides essential guidance to information system managers, information security managers, system designers and developers on implementing cryptographic controls at the information systems level to facilitate compliance with applicable regulatory requirements.

ENG 126**Essential Security Maintenance Policies**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls.

ENG 127**Essential Media Protection**

Duration: 15 minutes

This course provides essential guidance to individuals with information security implementation and operational responsibilities for developing and disseminating an organization-wide information media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities to facilitate compliance with applicable regulatory requirements.
