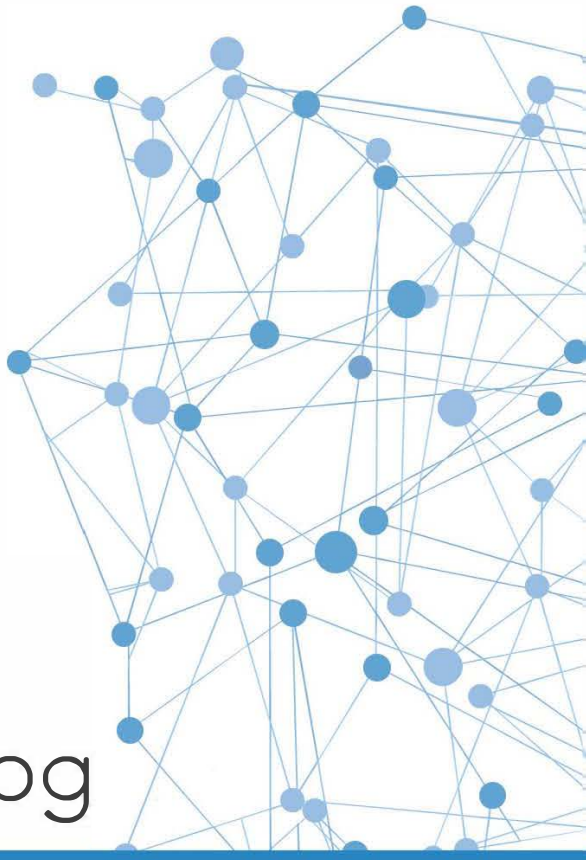
SECURITY INNOVATION



Training Program Catalog

All Courses

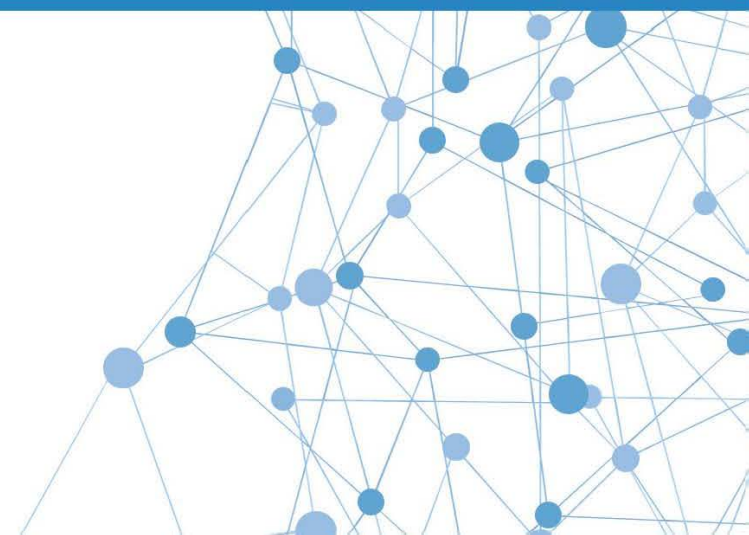


Table of Contents

Computer Based Training - Security Awareness - General Staff

Computer Based Training - Secure Coding

Computer Based Training - Secure Design

Computer Based Training - DevSecOps

Computer Based Training - Secure Engineering

Computer Based Training - Security Testing

Security Essentials

AWA 007
Information Privacy and Security Awareness for Executives
Duration: 45 minutes

This course provides decision-makers and managers with a concise summary of essential Information Security and Privacy Awareness requirements. Content is aligned with the topics contained in our standard Information Security and Privacy Awareness 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 course 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 to 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: 30 minutes

In this course, you will gain a fundamental understanding of application security and the important role it plays in meeting compliance requirements and managing risk. Coverage includes the three tenets of the (CIA) triad, confidentiality, integrity, and availability. After completing this course, you will be able to understand what application security is and understand the technical, business, and regulatory drivers for application security. You will also be able to identify key attacker motives, important security risk management terms and concepts, and key approaches for managing application security risk.

AWA 102
Secure Software Concepts
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 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.

Fundamentals of SDLC Security Series

This series 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 all phases of the software development lifecycle.

COD 102
The Role of Software Security
Duration: 10 minutes

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

COD 103
Creating Software Security Requirements
Duration: 10 minutes

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

COD 104
Designing Secure Software
Duration: 15 minutes

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

COD 105
Secure Software Development
Duration: 20 minutes

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

COD 106
The Importance of Software Integration and Testing
Duration: 15 minutes

This course introduces you to the integration and testing phases of the the software development lifecycle, including the roles of code review, fault injection, vulnerability scanning, penetration testing, and static analysis.

COD 107
Secure Software Deployment
Duration: 10 minutes

This course introduces you to the deployment phase of the software development lifecycle, which includes adhering to application security principles, defending critical software infrastructure such as the operating system, web servers, and databases, and creating a security incident response plan.

COD 108
Software Operations and Maintenance
Duration: 10 minutes

In this course, you will learn about application security patching, security misconfiguration and excessive attack surface, as well as insufficient logging and monitoring. You will also learn best practices for logging and different ways to defend the Operating System, Web Server, and the database.

COD 110
Fundamentals of Secure Mobile Development
Duration: 45 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 Database Security UPDATED
Duration: 30 minutes

In practice, database exploitation is the goal of many attackers, as it stores valuable information. 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 describes how to apply authentication and access control to your database and provides an understand of database privileges and limiting data access. Content coverage also includes techniques for protecting the database and methods for securely concealing specific data while providing an introduction to cloud databases and database encryption.

COD 152
Fundamentals of Secure Cloud Development
Duration: 20 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 160
Fundamentals of Secure Embedded Software Development UPDATED
Duration: 45 minutes

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

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.

Creating Secure C Code Series

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 security 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.

Creating Secure C++ Code Series

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 the use of:

- Standard containers and their built-in functions to avoid direct memory operations
- Bounds-checking functions, especially for string manipulation, to avoid buffer overflows
- Smart pointers to avoid memory leaks associated with managing raw pointers
- Standard concurrency features to help reduce the risk of introducing race conditions
- Object-oriented programming features to define and manipulate data in terms of objects, thus avoiding direct memory operations that may lead to memory corruption
- Range-based loops to avoid off-by-one indexing errors
- 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 presents 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++
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 214
Creating Secure GO Applications
Duration: 30 minutes

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

Creating Secure Code .NET Framework Foundations Series

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)
Duration: 30 minutes

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
Duration: 45 minutes

This course provides you with secure coding techniques and best practices that will help 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 presents 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.

IoT Specialization Series

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

This course provides an overview of and guidance for threats to IoT web interfaces, including overexposed ports, vulnerable default passwords, account enumeration, multiple authentication attempts, Cross-Site Scripting, Cross-Site Request Forgery, SQL Injection, and Command Injection.

COD 226
Insecure IoT Authentication and Authorization
Duration:10 minutes

In this course, you will learn best practices for implementing authentication and authorization for the Internet of Things.

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, including changing default credentials, protecting credentials in transit and in memory, using multi-factor authentication, preventing account enumeration, and detecting jailbreaking and tampering.

COD 230
Insecure IoT Firmware
Duration: 10 minutes

After you have completed this course, you will understand the steps of a typical update process, describe how to protect update connections, explain how to protect the update server, list the steps to securely sign and verify an update, evaluate whether Secure Boot is necessary for your device at this time, and identify types of sensitive data that should not be included in updates.

OWASP Mobile Series

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
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 understand 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.

PCI Compliance for Developers Series

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 series 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 246
PCI DSS 3: Protecting Stored Cardholder Data
Duration:15 minutes

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

---

COD 247
PCI DSS 4: Encrypting Transmission of Cardholder Data
Duration: 15 minutes

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

COD 248

PCI DSS 6: Develop and Maintain Secure Systems and Applications
Duration: 15 minutes

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

COD 249

PCI DSS 11: Regularly Test Security Systems and Processes
Duration: 15 minutes

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job. Vulnerabilities are being discovered continually by malicious individuals and researchers and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

COD 251

Defending AJAX- enabled Web Applications
Duration: 25 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 course, 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 253

Creating Secure AWS Cloud Applications
Duration: 45 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: 45 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 them. 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 understand the 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 UPDATED
Duration: 45 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 UPDATED
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 258
Creating Secure PHP Applications
Duration: 30 minutes

This course teaches PHP programmers the security principles they need to know to build secure PHP applications. It covers 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 259
Node.js Threats and Vulnerabilities
Duration: 30 minutes

This course covers 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

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 types of denial of service issues that commonly affect scripts.

COD 262

Fundamentals of Shell and Interpreted Language Security
Duration: 30 minutes

In this course, you will learn how shell scripting languages compare with modern interpreted languages, several information security principles like least privilege and defense in depth, the importance of data validation, and techniques for system hardening. You will also learn how to use filesystem operations safely to protect files, preventing or mitigating cached secret disclosure, the importance of up-to-date communication security techniques, and operating system portability issues.

COD 263

Secure Bash Scripting
Duration: 15 minutes

In this course, you will learn techniques for using Bash security settings, using quotation marks and double dash correctly in Bash, setting default file permissions, protecting temporary files, canonicalizing paths, preventing command injection, handling errors in Bash scripts, and using crontab

---

COD 264

Secure Perl Scripting
Duration: 15 minutes

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

COD 265

Secure Python Scripting
Duration: 15 minutes

In this course, you will learn important concepts for secure Python scripting, including validating command-line parameters, using quotation marks correctly, techniques for error and exception handling, using unmask to set default file permissions, protecting files, canonicalizing paths, avoiding uncontrolled format string vulnerabilities, preventing or mitigating several common injection vulnerabilities, defending against Regular Expression Denial of Service (DoS) attacks, and protecting sensitive data in transit.

COD 266

Secure Ruby Scripting
Duration: 15 minutes

In this course, you will learn important concepts for secure Ruby scripting, including validating command-line parameters, using quotation marks correctly, techniques for error and exception handling, using umask to set default file permissions, protecting files, canonicalizing paths, avoiding uncontrolled format string vulnerabilities, preventing or mitigating several common injection vulnerabilities, defending against Regular Expression Denial of Service (DoS) attacks, and protecting sensitive data in transit.

COD 267

Securing Python Microservices
Duration: 30 minutes

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

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

---

Creating Secure Java Series

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 JavaOS 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: 45 minutes

In this course, you will learn about the cryptographic functionality provided by the Java JCA Framework. It covers pseudo-random number generators, cryptographic hashing, and key derivation, generators and factories, Symmetric cryptography, cipher modes, and message authentication codes are discussed with examples. Asymmetric cryptography, certificates, key stores, and key agreements are also covered.

COD 284
Secure Java Coding
Duration: 30 minutes

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

Protecting C Code Series

This series provides C developers with the knowledge 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 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

---

Creating Secure ASP.NET MVC Applications Series

In this series, 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 learn about the Web API pipeline and how to implement authentication and authorization in Web API applications.

COD 308

Common ASP.NET MVC Vulnerabilities & Attacks

Duration: 45 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 understand the Web API pipeline and how to implement authentication and authorization in Web API applications.

COD 309

Securing ASP.NET MVC Applications
Duration: 30 minutes

This course teaches the fundamentals of authentication and authorization in ASP.NET Web API, and the roles they play in the OWIN pipeline. After completing this course, you will understand the Web API pipeline and where each component sits on that path, have a solid understanding of authentication and authorization filters and the role of each in your Web API application, and understand different authentication options and how to implement them in your application. You will also understand the importance of secure communication and the use of Transport Layer Security (TLS)to create secure data exchange tunnels.

COD 316

Creating Secure iOS Code in Objective C
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: 45 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: 45 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.

Protecting C# Series

This series describes methods that will produce secure C# applications. It presents the common security vulnerabilities like "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
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
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. After completing 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#
Duration: 25 minutes

This course describes protecting data both in transit and at rest in C# applications using strong cryptography. Examples illustrate how sensitive data can be protected in memory with the Secure String and Protected Memory 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 JavaScript and jQuery Code
Duration: 45 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.

Creating Secure HTML5 Code Series

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
Duration: 15 minutes

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, threats to user privacy, and techniques for mitigating these threats.

COD 362
HTML5 Built-In Security Features
Duration: 20 minutes

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
Duration: 20 minutes

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
Duration: 20 minutes

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

Protecting Java Code Series

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
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
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
Duration: 30 minutes

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

COD 383
Protecting Java Backend Services
Duration: 30 minutes

Backends are designed for applications that need faster performance, large amounts of addressable memory, and continuous or long-running background processes. The versatility of Java enables developers to design and deliver right business solutions however their efficiency requires distinctive experience and great expertise. This course provides developers and DevOps Engineers with next level understanding of best practices for developing back end frameworks using Java while developing skills necessary to handle user input and build secure systems.

DES 101

Fundamentals of Secure Architecture UPDATED

Duration: 20 minutes

In the past, software applications were created with little thought to the importance of security. This course introduces some of the biggest security disasters in software design and what lessons can be learned from them. Participants will develop a fundamental understand of the concepts of security architecture, its design, and the kinds of models, policies, correspondence, structure testing, and permissions that should be implemented. Lastly, they will understand and use confidentiality, integrity, and availability as the three main tenets of information security.

DES 151

Fundamentals of the PCI Secure SLC Standard NEW

Duration: 25 minutes

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

Fundamentals of Cryptography Series

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

Duration: 45 minutes

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

Duration: 15 minutes

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, andK0019: Knowledge of cryptography and cryptographic key management concepts.

DES 204

The Role of Cryptography in Application Development

Duration: 15 minutes

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

Duration: 45 minutes

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 210

Hardening Linux/Unix Systems COMING SOON

Duration: 30 minutes

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

DES 212

Architecture Risk Analysis and Remediation UPDATED

Duration: 30 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.

Secure Enterprise Infrastructure Series

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 with all topics covered in alignment to NICE framework.

DES 214

Securing Infrastructure Architecture

Duration: 30 minutes

This course is designed for Network Operations Specialists and aligns with the NICE requirements for the secure planning, implementation and operation of network services and systems, including hardware and virtual environments. Coverage includes: Security Principles, Network Topologies, Demilitarized Zones, Routers, Switches, Bridges, Firewalls, Wireless Access Points, Transmission Media, and Network Authentication Servers Configuration.

DES 215

Defending Infrastructure

Duration: 30 minutes

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

DES 216
Protecting Cloud Infrastructure
Duration: 40 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 218
Protecting Microservices, Containers, and Orchestration
Duration: 30 minutes

Using Microservices, organizations can isolate software functionality into multiple independent modules that are individually responsible for performing precisely defined, standalone tasks communicating with each other through simple, universally accessible application programming interfaces (APIs). Containers enable developers to simultaneously build and ship these microservices; integrate them with other systems and automatically orchestrate them using predefined rules and processes. This course educates DevOps Engineers, IT Architects, and Network Engineers working in Linux or on the cloud to add value to application lifecycle through proper orchestration and enable faster development and fault-prone provisioning and configurations.

Applying OWASP 2017 Mitigations Series

The primary objective of this series of courses, and of the OWASP Top 10, is to educated 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 Injection.

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 255
Securing the IoT Update Process NEW
Duration: 30 minutes

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

DES 260
Fundamentals of IoT Architecture and Design
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.

Blockchain Security Series COMING SOON

Blockchain offers a high level of security because it is decentralized, offers encryption and validation, provides transparency, and is conceptually difficult to hack. Blockchain based networks can be used to prevent cyber-attacks by being; a trusted system, immutable and by network consensus. This series provides essential guidance for organizations regardless of their adoption of the technology; whether they are looking to create a secure network or secure existing blockchain assets.

DES 305

Protecting Existing Blockchain Assets COMING SOON
Duration: 20 minutes

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

DES 306

Creating a Secure Blockchain Network COMING SOON
Duration: 20 minutes

While Blockchain technology continues to emerge due to its ability to improve data security, accelerate transactions and save costs, it comes with its advantages it comes with a wide array of challenges. Properly securing a blockchain network begins with the implementation of strong authentication and cryptography key vaulting mechanisms. This course provides learners with an understanding of the essential requirements for creating a secure blockchain network.

DES 311

Creating Secure Application Architecture UPDATED
Duration: 45 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.

DSO 201

Fundamentals of Secure DevOps NEW
Duration: 30 minutes

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

DSO 205

Securing the COTS Supply Chain COMING SOON
Duration: 15 minutes

While the use of Commercial-off-the-shelf software (COTS) helps expand functionality and productivity, it also carries inherent complexities. Unfortunately, it is rare for acquisition approaches to account for complex software supply chains; this course provides learners with an understand of how to apply DevSecOps best practices to reduce software supply chain risks.

DSO 253

DevSecOps in the AWS Cloud COMING SOON
Duration: 20 minutes

The cloud platform helps solve distributed complexity issues and provides DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. This course demonstrates how to align and configure AWS services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

DSO 254

DevSecOps in the Azure Cloud COMING SOON
Duration: 20 minutes

Using a cloud Platform solves for issues with distributed complexity and provide DevOps automation with a standard and centralized platform for testing, deployment, and production creating a complementary relationship between the two. provides learners with an understanding of how to align and configure Azure services to NIST Cybersecurity Framework (CSF) core functions to achieve security in the cloud.

ENG 150
Meeting Confidentiality, Integrity, and Availability Requirements
Duration: 30 minutes

The CIA Triad - Confidentiality, Integrity, and Availability - are the information security tenets used as a means of analyzing and improving the security of your application and its data.

Implementing the MS SDL Process Into your SDLC Series

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
Duration: 25 minutes

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
Duration: 20 minutes

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
Duration: 12 minutes

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

ENG 194
Implementing MS SDL Line of Business
Duration: 20 minutes

This course describes the Microsoft Security Development Life cycle 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 life cycle phases: Requirements, Design, Implementation, Verification, and Release.

ENG 195
Implementing the MS SDL Threat Modeling Tool
Duration: 20 minutes

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 UPDATED
Durations: 45 minutes

Threat modeling is a structured activity for identifying and evaluating application threats and vulnerabilities. In this course, you will learn how to quickly create a basic threat model for your application scenario that can be used to help refine application design through all stages of development and serve as a central reference among teams. Additionally, this course will introduce the five steps of the threat modeling process and the tasks performed in each step while teaching learners how to adapt the process to their own situation.

ENG 211

How to Create Application Security Design Requirements UPDATED

Duration: 15 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 251

Risk Management Foundations NEW

Durations: 20 minutes

Risk Management should be a foundational tool used to facilitate thoughtful and purposeful defense strategies. In today's environment, the most significant threats to systems come from purposeful attacks that are often disciplined, well organized, and well-funded. This course helps IT Architects, Analysts, and DevOps Engineers to understand their responsibilities when protecting organizational assets.

ENG 311

Attack Surface Analysis & Reduction UPDATED

Duration: 25 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 UPDATED

Duration: 30 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.

Risk Management Framework Series

The Risk Management Framework can add value to any organization regardless of the industry sector or size of the company, but adoption of this framework consists of crucial components that must not be overlooked. This series provides various roles across the organization with essential knowledge necessary to carry out all steps which help an organization select the appropriate security controls to protect against resource, asset, and operational risk. This includes categorization of systems and information; selection, implementation and assessment of security controls; authorization of system operation; and monitoring and assessment of selected controls.

ENG 351

Preparing the Risk Management Framework NEW
Duration: 20 minutes

Before any organization can adequately implement the risk management framework they must understand how to determine and apply appropriate security requirements. Preparation requires a disciplined and structured set of activities in order to execute the framework at the appropriate risk management levels. This course provides Engineers, Software Architects, and Systems Analysts with context and priorities for managing security and privacy risk.

ENG 352

Categorizing Systems and Information within the RMF COMING SOON
Duration: 10 minutes

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

ENG 353

Selecting, Implementing and Assessing Controls within the RMF COMING SOON
Duration: 20 minutes

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

ENG 354

Authorizing and Monitoring System Controls within the RMF COMING SOON
Duration: 20 minutes

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

TST 101
Fundamentals of Security Testing
Duration: 20 minutes

In this course you will learn about the different fundamental types of security testing. By the end of this course you will understand threat modeling, how threat modeling applies in the design phase of the SDLC, approaches to threat modeling, vulnerability scanning, penetration testing, static analysis pros and cons, code review pros and cons.

TST 202
Penetration Testing Fundamentals NEW
Duration: 25 minutes

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

TST 205
Performing Vulnerability Scans NEW
Duration: 45 minutes

Performing vulnerability scans is necessary to evaluate the security of an organization's network and help protect organizational data and assets. This includes assessing, mitigating and reporting on any security vulnerabilities that exist in an organization's systems and software. This course will provide DevOps Engineers, Network Engineers, QA Test Engineers, and Operations/IT Managers with an understanding of how to perform vulnerability scans.

Testing for OWASP 2017 Series

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
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
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

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

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

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

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

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

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

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

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.

Testing for CWE SANS Top 25 Software Errors Series

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 on-line resources.

TST 251

Testing for SQL Injection

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

In this course, you will learn how to identify and mitigate CWE-601: Open Redirect. Coverage includes techniques for spotting CWE-601 vulnerabilities through coder eview 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

Duration: 15 minutes

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

Duration: 15 minutes

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

Duration: 15 minutes

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.

TST 301

Infrastructure Penetration Testing COMING SOON

Duration: 45 minutes

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

TST 302

Application Penetration Testing COMING SOON

Duration: 45 minutes

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

Penetration Testing Series for Common Vulnerabilities and Attack Vectors NEW

Penetration testing examines the real-world effectiveness of security controls and processes around networks and applications against real world attacks. This series provides guidance and necessary knowledge of techniques to exploit common vulnerabilities and attack surfaces to determine whether unauthorized access or other malicious activity is possible.

TST 351

Penetration Testing for TLS Vulnerabilities NEW
Duration: 12 minutes

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

TST 352

Penetration Testing for Injection Vulnerabilities NEW
Duration: 12 minutes

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

TST 353

Penetration Testing for SQL Injection NEW
Duration: 12 minutes

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

TST 354

Penetration Testing for Memory Corruption Vulnerabilities NEW
Duration: 12 minutes

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

TST 355

Penetration Testing for Authorization Vulnerabilities NEW
Duration: 12 minutes

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

TST 356

Penetration Testing for XSS NEW
Duration: 12 minutes

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

TST 357

Penetration Testing for Hardcoded Secrets NEW
Duration: 12 minutes

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

TST 358

Penetration Testing Wireless Networks NEW
Duration: 12 minutes

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

TST 359

Penetration Testing Network Infrastructure NEW
Duration: 12 minutes

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

TST 360

Penetration Testing for Authentication Vulnerabilities NEW
Duration: 12 minutes

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

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.
