LEARNING PATHS

Application Security Role-Based Curriculum
<table>
<thead>
<tr>
<th>Role</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Analyst</td>
<td>2</td>
</tr>
<tr>
<td>Business Analyst</td>
<td>2</td>
</tr>
<tr>
<td>Software Architect</td>
<td>2</td>
</tr>
<tr>
<td>Embedded Architect</td>
<td>2</td>
</tr>
<tr>
<td>IT Architect</td>
<td>2</td>
</tr>
<tr>
<td>Embedded QA/Test Engineer</td>
<td>2</td>
</tr>
<tr>
<td>Automation Engineer</td>
<td>2</td>
</tr>
<tr>
<td>DevOps Engineer</td>
<td>2</td>
</tr>
<tr>
<td>Network Engineer</td>
<td>2</td>
</tr>
<tr>
<td>IT Architect</td>
<td>2</td>
</tr>
<tr>
<td>Embedded Architect</td>
<td>2</td>
</tr>
<tr>
<td>Software Architect</td>
<td>2</td>
</tr>
<tr>
<td>Business Analyst</td>
<td>2</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>2</td>
</tr>
<tr>
<td>.NET Developer</td>
<td>3</td>
</tr>
<tr>
<td>Android Developer</td>
<td>3</td>
</tr>
<tr>
<td>Back-End Web Developer</td>
<td>3</td>
</tr>
<tr>
<td>C Developer</td>
<td>3</td>
</tr>
<tr>
<td>C# Developer</td>
<td>3</td>
</tr>
<tr>
<td>C++ Developer</td>
<td>3</td>
</tr>
<tr>
<td>Front-End Developer</td>
<td>3</td>
</tr>
<tr>
<td>HTML5 Developer</td>
<td>3</td>
</tr>
<tr>
<td>iOS Developer</td>
<td>3</td>
</tr>
<tr>
<td>Java Developer</td>
<td>3</td>
</tr>
<tr>
<td>JavaScript Developer</td>
<td>3</td>
</tr>
<tr>
<td>Mobile Developer</td>
<td>3</td>
</tr>
<tr>
<td>PHP Developer</td>
<td>3</td>
</tr>
<tr>
<td>Python Web Developer</td>
<td>3</td>
</tr>
<tr>
<td>Ruby on Rails Developer</td>
<td>3</td>
</tr>
<tr>
<td>Web Developer</td>
<td>3</td>
</tr>
<tr>
<td>Node.js Developer</td>
<td>3</td>
</tr>
<tr>
<td>Swift Developer</td>
<td>3</td>
</tr>
<tr>
<td>Microsoft SDL</td>
<td>3</td>
</tr>
<tr>
<td>Cloud Developer</td>
<td>3</td>
</tr>
<tr>
<td>PCI Developer</td>
<td>3</td>
</tr>
<tr>
<td>Embedded Developer</td>
<td>3</td>
</tr>
<tr>
<td>Core Developer</td>
<td>3</td>
</tr>
<tr>
<td>DevOps Engineer</td>
<td>3</td>
</tr>
<tr>
<td>Network Engineer</td>
<td>3</td>
</tr>
<tr>
<td>Automation Engineer</td>
<td>3</td>
</tr>
<tr>
<td>Embedded QA/Test Engineer</td>
<td>3</td>
</tr>
<tr>
<td>Quality Assurance (QA)/Test Engineer</td>
<td>3</td>
</tr>
<tr>
<td>IT Architect</td>
<td>3</td>
</tr>
<tr>
<td>Embedded Architect</td>
<td>3</td>
</tr>
<tr>
<td>Software Architect</td>
<td>3</td>
</tr>
<tr>
<td>Business Analyst</td>
<td>3</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>3</td>
</tr>
<tr>
<td>.NET Developer</td>
<td>4</td>
</tr>
<tr>
<td>Android Developer</td>
<td>4</td>
</tr>
<tr>
<td>Back-End Web Developer</td>
<td>4</td>
</tr>
<tr>
<td>C Developer</td>
<td>4</td>
</tr>
<tr>
<td>C# Developer</td>
<td>4</td>
</tr>
<tr>
<td>C++ Developer</td>
<td>4</td>
</tr>
<tr>
<td>Front-End Developer</td>
<td>4</td>
</tr>
<tr>
<td>HTML5 Developer</td>
<td>4</td>
</tr>
<tr>
<td>iOS Developer</td>
<td>4</td>
</tr>
<tr>
<td>Java Developer</td>
<td>4</td>
</tr>
<tr>
<td>JavaScript Developer</td>
<td>4</td>
</tr>
<tr>
<td>Mobile Developer</td>
<td>4</td>
</tr>
<tr>
<td>PHP Developer</td>
<td>4</td>
</tr>
<tr>
<td>Python Web Developer</td>
<td>4</td>
</tr>
<tr>
<td>Ruby on Rails Developer</td>
<td>4</td>
</tr>
<tr>
<td>Web Developer</td>
<td>4</td>
</tr>
<tr>
<td>Node.js Developer</td>
<td>4</td>
</tr>
<tr>
<td>Swift Developer</td>
<td>4</td>
</tr>
<tr>
<td>Microsoft SDL</td>
<td>4</td>
</tr>
<tr>
<td>Cloud Developer</td>
<td>4</td>
</tr>
<tr>
<td>PCI Developer</td>
<td>4</td>
</tr>
<tr>
<td>Embedded Developer</td>
<td>4</td>
</tr>
<tr>
<td>Core Developer</td>
<td>4</td>
</tr>
<tr>
<td>DevOps Engineer</td>
<td>4</td>
</tr>
<tr>
<td>Network Engineer</td>
<td>4</td>
</tr>
<tr>
<td>Automation Engineer</td>
<td>4</td>
</tr>
<tr>
<td>Embedded QA/Test Engineer</td>
<td>4</td>
</tr>
<tr>
<td>Quality Assurance (QA)/Test Engineer</td>
<td>4</td>
</tr>
<tr>
<td>IT Architect</td>
<td>4</td>
</tr>
<tr>
<td>Embedded Architect</td>
<td>4</td>
</tr>
<tr>
<td>Software Architect</td>
<td>4</td>
</tr>
<tr>
<td>Business Analyst</td>
<td>4</td>
</tr>
<tr>
<td>Systems Analyst</td>
<td>4</td>
</tr>
<tr>
<td>Role</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Systems Administrator</td>
<td>34</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>35</td>
</tr>
<tr>
<td>Linux Administrator</td>
<td>36</td>
</tr>
<tr>
<td>Application/Product Owner</td>
<td>36</td>
</tr>
<tr>
<td>Project Manager</td>
<td>37</td>
</tr>
<tr>
<td>Cyber Security Professional</td>
<td>38</td>
</tr>
<tr>
<td>Operations/IT Manager</td>
<td>38</td>
</tr>
<tr>
<td>Application Security Champion</td>
<td>39</td>
</tr>
<tr>
<td>Information Security Specialist</td>
<td>39</td>
</tr>
<tr>
<td>Systems Leadership</td>
<td>40</td>
</tr>
<tr>
<td>Development Manager</td>
<td>41</td>
</tr>
</tbody>
</table>
.NET Developer
Details 45 Courses, 25 Hours, 30 CPE Credits

Core
Designed to provide an understanding of security principles and best practices for developing secure .NET applications. The path focuses on fundamentals of application security, application security risk management, and common vulnerabilities in an application.

Courses Include
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- COD 261 Threats to Scripts
- COD 262 Fundamentals of Shell and Interpreted Language Security
- ENG 205 Fundamentals of Threat Modeling

Advanced
Covers key concepts of cryptography and creating secure code for .NET applications. This path aims to educate learners about the OWASP Top 10 focusing on consequences of these application security weaknesses while enabling them to develop secure code and mitigate security vulnerabilities.

Courses Include
- COD 251 Creating Secure AJAX Code – ASP.NET Foundations
- COD 255 Creating Secure Code – Web API Foundations
- COD 311 Creating Secure Code ASP.NET MVC Applications
- COD 321-323 Protecting # Code Series (3)
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 222-231 Applying OWASP 2017 Mitigation Series (10)

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling using the Microsoft Security Development Lifecycle (SDL) process. Developers 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, and guidelines for secure source code review.

Courses Include
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

Android Developer
Details 39 Courses, 20 Hours, 24 CPE Credits
Core

Designed to provide an understanding of security principles, best practices for developing secure mobile applications, and essential access control on mobile devices. The Learning Path also focuses on fundamentals of application security, application security risk management, and common vulnerabilities in a mobile application.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 110 Fundamentals of Secure Mobile Development
- DES 260 Fundamentals of IoT Architecture and Design
- ENG 112 Essential Access Control for Mobile Devices
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers key fundamentals of mobile application threats and mitigations, mobile data cryptography, and creating secure code for Android applications. This path also covers Mobile OWASP Top 10, to educate learners about the consequences of the most common and most important application security weaknesses to enable the learner to develop secure code and mitigate security vulnerabilities.

Courses Include

- COD 229 Insecure IoT Mobile Interface
- COD 234-237 Mobile OWASP Top 10 Series (4)
- COD 318 Creating Secure Android Code in Java
- DES 202-205 Fundamentals of Cryptography Series (4)
- TST 252 Testing for OS Command Injection
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 270 Testing for Incorrect Calculation of Buffer Size
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling using the Microsoft Security Development Lifecycle (SDL) process. Developers will learn to define the attack surface of an application and how to reduce the risk to a mobile application by minimizing the application’s attack surface, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
Back-End Web Developer
Details 29 Courses, 18 Hours, 22 CPE Credits

Core
Designed to provide an understanding of security principles, best practices for writing secure server-side code, and security issues and challenges specific to AJAX applications.

Courses Include
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code

Advanced
Covers key fundamentals of security features needed to write web services and API's used by front-end and mobile application developers.

Courses Include
- COD 241 Creating Secure Oracle Database Applications
- COD 251 Creating Secure AJAX Code – ASP.NET Foundations
- COD 252 Creating Secure AJAX Code – Java Foundations
- COD 253 Creating Secure Creating Secure AWS Cloud Applications
- COD 254 Creating Secure Azure Applications
- COD 255 Creating Secure Code – Web API Foundations
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure
- DES 227 Applying OWASP 2017 Mitigating Security Misconfiguration
- TST 224 Testing for OWASP 2017 Sensitive Data Exposure
- TST 227 Testing for OWASP 2017 Security Misconfiguration

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. Developers will learn to define the attack surface of an application and how to reduce the risk to back-end applications by minimizing the attack surface, and guidelines for secure source code review.

Courses Include
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

C Developer
Details 43 Courses, 20 Hours, 24 CPE Credits

Core
Designed to provide an understanding of security principles and best practices for developing secure C applications. The path focuses on fundamentals of application security, application security risk management, and common vulnerabilities in an application.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- **COD 102-108 Fundamentals of SDLC Security Series (7)**
- COD 261 Threats to Scripts

**Advanced**

Covers key concepts of Transport Layer Security (TLS), encrypted network communications, Run-Time Protection, buffer overflow mitigations and memory management using C code. This path also highlights common C vulnerabilities and attacks and key concepts of cryptography and will enable the learner to develop secure code and mitigate security vulnerabilities.

**Courses Include**

- COD 201-202 Creating Secure C Code Series (2)
- COD 301-303 Protecting C Code Series (3)
- **DES 202-205 Fundamentals of Cryptography Series (4)**
- TST 255 Testing for Missing Authentication for Critical Function
- TST 257 Testing for use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance of Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect
- TST 273 Testing for Uncontrolled Format String

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- **ENG 191-195 Integrating the MS SDL into your SDLC Series (5)**
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review
C# Developer
Details 31 Courses, 18 Hours, 21 CPE Credits

Core
Designed to provide an understanding of security principles and best practices for developing secure C# applications. The path focuses on fundamentals of application security, application security risk management, and common vulnerabilities in an application.

Courses Include
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)

Advanced
Provides a thorough grounding of security features necessary to develop modern applications that run on desktops or back-end processes powering modern web applications. Covers secure coding best practices that enable learners to build secure enterprise systems, desktop applications, websites and mobile applications. Users will also understand how to develop scalable applications using multithreading features of .NET framework.

Courses Include
- COD 225 Insecure IoT Web Interfaces
- COD 311 Creating Secure Code ASP.NET MVC Applications
- COD 321-323 Protecting C# Series (3)
- DES 202-205 Fundamentals of Cryptography Series (4)

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

C++ Developer
Details 45 Courses, 20 Hours, 23 CPE Credits

Core
Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- **COD 102-108 Fundamentals of SDLC Security Series (7)**
- COD 262 Fundamentals of Shell and Interpreted Language Security
- ENG 205 Fundamentals of Threat Modeling

**Advanced**

Covers key concepts for creating secure C++ applications, implementing data protection techniques in C++ applications. It also covers key concepts of cryptography and enables developers to develop secure C++ code.

**Courses Include**

- **COD 206-207, 307 Creating Secure C++ Code Series**
- COD 263 Secure Bash Scripting
- COD 264 Secure Perl Scripting
- COD 265 Secure Python Scripting
- COD 266 Secure Ruby Scripting
- **DES 201-205 Fundamentals of Cryptography Series**
- TST 255 Testing for Missing Authentication for Critical Function
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code Without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect
- TST 273 Testing for Uncontrolled Format String

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- **ENG 191-195 Integrating the MS SDL into your SDLC Series (5)**
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review
Front-End Developer
Details 45 Courses, 25 Hours, 30 CPE Credits

Core
Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- ENG 205 Fundamentals of Threat Modeling

Advanced
Covers how vulnerabilities are discovered and exploited and provides a solid foundation for using markup languages, design and client-side scripts and framework to create secure environments for everything that users touch. It also covers key concepts of cryptography and enables developers to build a strong line of defense and provides a deep understanding of HTML5, CSS and responsive web development.

Courses Include
- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails
- COD 259 Node.js Threats and Vulnerabilities
- COD 315 Creating Secure PHP Code
- COD 352 Creating Secure jQuery Code
- COD 361-364 Creating Secure HTML5 Code Series (4)
- DES 201-205 Fundamentals of Cryptography Series
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review
HTML5 Developer
Details 43 Courses, 26 Hours, 31 CPE Credits

Core
Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- **COD 102-108 Fundamentals of SDLC Security Series (7)**
- COD 153 Fundamentals of Secure AJAX Code
- ENG 205 Fundamentals of Threat Modeling

Advanced
Covers how to infuse software security into the development lifecycle and provides a solid foundation of HTML5 security features to help build applications with a strong line of defense. Front-end developers will develop a working knowledge of ASP.net, SWL, high-level scripting languages, version control and CMS systems.

Courses Include
- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails
- COD 259 Node.js Threats and Vulnerabilities
- **COD 281-284 Creating Secure Java Code Series (3)**
- COD 311 Creating Secure Code ASP.NET MVC Applications
- COD 352 Creating Secure jQuery Code
- **COD 361-364 Creating Secure HTML5 Code Series (4)**
- DES 201-205 Fundamentals of Cryptography Series
- DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure
- DES 228 Applying OWASP 2017 Mitigating Cross-Site Scripting
- TST 224 Testing for OWASP 2017 Sensitive Data Exposure
- TST 228 Testing for OWASP 2017 Cross-Site Scripting

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- **ENG 191-195 Integrating the MS SDL into your SDLC Series (5)**
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review
iOS Developer

Details 39 Courses, 20 Hours, 25 CPE Credits

Core

Designed to provide an understanding of security principles, best practices for developing secure mobile applications, and essential access control on mobile devices. The Learning Path also focuses on fundamentals of application security, application security risk management, and common vulnerabilities in mobile applications.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 110 Fundamentals of Secure Mobile Development
- DES 260 Fundamentals of IoT Architecture and Design
- ENG 112 Essential Access Control for Mobile Devices
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers key fundamentals of iOS application threats and mitigations, mobile data cryptography, and creating secure code for iOS applications. This path also covers Mobile OWASP Top 10, to educate learners about the consequences of the most common and most important application security weaknesses to enable the learner to develop secure code and mitigate security vulnerabilities.

Courses Include

- COD 229 Insecure IoT Mobile Interface
- COD 234-237 Mobile OWASP Top 10 Series (4)
- COD 316 Creating Secure iOS Code in Objective C
- COD 317 Creating Secure iOS Code in Swift
- DES 202-205 Fundamentals of Cryptography Series (4)
- TST 252 Testing for OS Command Injection
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 270 Testing for Incorrect Calculation of Buffer Size
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling using the Microsoft Security Development Lifecycle (SDL) process. Developers 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, and guidelines for source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
Java Developer

Details 58 Courses, 27 Hours, 33 CPE Credits

Core

Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers key concepts of Java Security Models, Java Authentication and Authorization Service to understand how to create secure java Code. This path also covers fundamentals of cryptography and related security issues in Java along with OWASP Top 10 and educates learners on the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks.

Courses Include

- COD 219 Creating Secure Code – SAP ABAP Foundations
- COD 225-230 IoT Specialization Series (6)
- COD 252 Creating Secure AJAX Code – Java Foundations
- COD 256 Creating Secure Code – Ruby on Rails
- COD 259 Node.js Threats and Vulnerabilities
- COD 281-284 Creating Secure Java Code Series (4)
- COD 361-364 Creating Secure HTML5 Code Series (4)
- DES 201-205 Fundamentals of Cryptography Series
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)
- COD 380-382 Protecting Java Code Series (3)

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include
JavaScript Developer

Details 46 Courses, 27 Hours, 33 CPE Credits

Core

Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers key concepts of protecting JavaScript and eliminating vulnerabilities while providing a solid understanding of common pitfalls and security flaws, fundamentals of Cryptography and related security issues. Developers are also educated on OWASP Top 10 and the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks.

Courses Include

- COD 241 Creating Secure Oracle Database Applications
- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails
- COD 259 Node.js Threats and Vulnerabilities
- COD 281-284 Creating Secure Java Code Series (3)
- COD 315 Creating Secure PHP Code
- COD 352 Creating Secure jQuery Code
- COD 361-364 Creating Secure HTML5 Code Series (4)
- DES 201-205 Fundamentals of Cryptography Series
- DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure
- DES 225 Applying OWASP 2017 Mitigating XML External Entities
- DES 228 Applying OWASP 2017 Mitigating Cross-Site Scripting
- TST 224 Testing for OWASP 2017 Sensitive Data Exposure
- TST 225 Testing for OWASP 2017 XML External Entities
- TST 228 Testing for OWASP 2017 Cross-Site Scripting

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat
modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

Mobile Developer

Details 44 Courses, 23 Hours, 28 CPE Credits

Core

Designed to provide an understanding of security principles, best practices for developing secure mobile applications, and essential access control on mobile devices. The Learning Path also focuses on fundamentals of application security, application security risk management, and common vulnerabilities in mobile applications.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 110 Fundamentals of Secure Mobile Development
- COD 261 Threats to Scripts
- DES 260 Fundamentals of IoT Architecture and Design
- ENG 112 Essential Access Control for Mobile Devices
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers key fundamentals of mobile application threats and mitigations, mobile data cryptography, and creating secure code for mobile applications. This path also covers Mobile OWASP Top 10, to educate learners about the consequences of the most common and most important application security weaknesses to enable the learner to develop secure code and mitigate security vulnerabilities.

Courses Include

- COD 229 Insecure IoT Mobile Interface
- COD 230 Insecure IoT Firmware
- COD 234-237 Mobile OWASP Top 10 Series (4)
- COD 316 Creating Secure iOS Code in Objective C
- COD 317 Creating Secure iOS Code in Swift
- COD 318 Creating Secure Android Code in Java
- DES 202-205 Fundamentals of Cryptography Series (4)
- TST 252 Testing for OS Command Injection
- TST 253 Testing for Classic Buffer Overflow
- TST 255 Testing for Missing Authorization
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 258 Testing for Missing Encryption of Sensitive Data
• TST 259 Testing for Unrestricted Upload of File with Dangerous Type
• TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
• TST 261 Testing for Execution with Unnecessary Privileges
• TST 264 Testing for Download of Code without Integrity Check
• TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
• TST 267 Testing for Incorrect Permission Assignment for Critical Resource
• TST 268 Testing for Use of a Potentially Dangerous Function
• TST 269 Testing for Use of Broken or Risky Cryptographic Algorithm
• TST 270 Testing for Incorrect Calculation of Buffer Size
• TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
• TST 272 Testing for Open Redirect
• TST 273 Testing for Uncontrolled Format String
• TST 275 Testing for Use of a One-Way Hash without a Salt

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling using the Microsoft Security Development Lifecycle (SDL) process. Developers 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, and guidelines for source code review.

Courses Include

• DES 101 Fundamentals of Secure Architecture
• DES 212 Architecture Risk Analysis and Remediation
• DES 311 Creating Secure Application Architecture
• ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
• ENG 211 How to Create Application Security Design Requirements
• ENG 311 Attack Surface Analysis & Reduction
• ENG 312 How to Perform a Security Code Review

PHP Developer

Details 60 Courses, 28 Hours, 33 CPE Credits

Core

Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

• AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• COD 102-108 Fundamentals of SDLC Security Series (7)
• COD 153 Fundamentals of Secure AJAX Code
• ENG 205 Fundamentals of Threat Modeling

Advanced

Covers key concepts of creating secure applications using Ruby on Rail Foundations, Python Web Applications, Python, Perl, PHP, HTML5, and jQuery. Highlighting key considerations for protecting sensitive data while scripting and providing insights into the fundamentals of cryptography. Developers are also educated on OWASP Top 10 and
the consequences of the most common and most important application security weaknesses to enable them to develop secure code and mitigate security vulnerabilities using common standards and frameworks.

Courses Include

- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails
- COD 259 Node.js Threats and Vulnerabilities
- COD 261-266 Secure Scripting Series (6)
- COD 281-284 Creating Secure Java Code Series (4)
- COD 315 Creating Secure PHP Code
- COD 361-364 Creating Secure HTML5 Code Series (4)
- DES 201-205 Fundamentals of Cryptography Series
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)
- TST 222-231 Testing for OWASP 2017 Series (10)

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

Python Web Developer

Details
47 Courses, 24 Hours, 29 CPE Credits

Core

Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- COD 261 Threats to Scripts
- COD 262 Fundamentals of Shell and Interpreted Language Security
- ENG 205 Fundamentals of Threat Modeling

Advanced
Covers key concepts of creating secure applications using AJAX code, Ruby on Rails Foundations, Python Web Applications, Python, Perl etc. It highlights key consideration to protecting sensitive data while scripting and give insights into the fundamentals of cryptography. Developers are also educated on OWASP Top 10 and the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks.

**Courses Include**

- COD 252 Creating Secure AJAX Code – Java Foundations
- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails
- COD 257 Creating Secure Python Web Applications
- COD 265 Secure Python Scripting
- COD 361-364 Creating Secure HTML5 Code Series (4)
- DES 201-205 Fundamentals of Cryptography Series
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

**Ruby on Rails Developer**

**Details** 43 Courses, 25 Hours, 30 CPE Credits

**Core**

Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- ENG 205 Fundamentals of Threat Modeling
Advanced

Covers best practices and techniques for writing server-side web application logic using Ruby, around the framework Rails while providing an understanding of the various types of vulnerabilities, building strong session management, and preventing common vulnerabilities in Rails applications.

Courses Include

- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails Foundations
- COD 257 Creating Secure Python Web Applications
- COD 259 Node.js Threats and Vulnerabilities
- COD 281-284 Creating Secure Java Code Series (3)
- COD 352 Creating Secure jQuery Code
- COD 361-364 Creating Secure HTML5 Foundations Series (2)
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure
- DES 228 Applying OWASP 2017 Mitigating Cross-Site Scripting
- TST 224 Testing for OWASP 2017 Sensitive Data Exposure
- TST 228 Testing for OWASP 2017 Cross-Site Scripting

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

Web Developer

Details 60 Courses, 31 Hours, 37 CPE Credits

Core

Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- COD 261 Threats to Scripts
• COD 262 Fundamentals of Shell and Interpreted Language Security
• ENG 205 Fundamentals of Threat Modeling

Advanced
Covers key concepts of creating secure applications using AJAX code, Ruby on Rails Foundations, Python Web Applications, Python, Perl, PHP, HTML5, and jQuery. This course also highlights key consideration to protect sensitive data while scripting and give insights of fundamentals of cryptography. Developers are also educated on OWASP Top 10 and the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks.

Courses Include
• COD 241 Creating Secure Oracle Database Applications
• COD 252 Creating Secure AJAX Code – Java Foundations
• COD 255 Creating Secure Code – Web API Foundations
• COD 256 Creating Secure Code – Ruby on Rails Foundations
• COD 257 Creating Secure Python Web Applications
• COD 259 Node.js Threats and Vulnerabilities
• COD 315 Creating Secure PHP Code
• COD 352 Creating Secure jQuery Code
• COD 361-364 Creating Secure HTML5 Foundations Series (2)
• DES 202-205 Fundamentals of Cryptography Series (4)
• DES 222-231 Applying OWASP 2017 Mitigations Series (10)
• TST 222-231 Testing for OWASP 2017 Mitigations Series (10)

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include
• DES 101 Fundamentals of Secure Architecture
• DES 212 Architecture Risk Analysis and Remediation
• DES 311 Creating Secure Application Architecture
• ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
• ENG 211 How to Create Application Security Design Requirements
• ENG 311 Attack Surface Analysis & Reduction
• ENG 312 How to Perform a Security Code Review

Node.js Developer
Details 55 Courses, 32 Hours, 38 CPE Credits

Essential
Provides learners with an understanding of security principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

www.securityinnovation.com | @SecInnovation | 978.694.1008
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 153 Fundamentals of Secure AJAX Code
- ENG 205 Fundamentals of Threat Modeling

**Professional**

Provides a solid foundation of security features necessary to code, test and operate Node.js based services and develops a working knowledge of web libraries, frameworks and the whole web stack while protecting data using secure coding best practices. Developers are also educated on OWASP Top 10 and the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks.

**Courses Include**

- COD 241 Creating Secure Oracle Database Applications
- COD 255 Creating Secure Code – Web API Foundations
- COD 256 Creating Secure Code – Ruby on Rails Foundations
- COD 257 Creating Secure Python Web Applications
- COD 259 Node.js Threats and Vulnerabilities
- COD 311 Creating Secure Code ASP.NET MVC Applications
- COD 315 Creating Secure PHP Code
- COD 352 Creating Secure jQuery Code
- COD 361-364 Creating Secure HTML5 Foundations Series (2)
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure
- DES 225 Applying OWASP 2017 Mitigating XML External Entities
- DES 228 Applying OWASP 2017 Mitigating Cross-Site Scripting
- TST 224 Testing for OWASP 2017 Sensitive Data Exposure
- TST 225 Testing for OWASP 2017 XML External Entities
- TST 228 Testing for OWASP 2017 Cross-Site Scripting

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Integrating the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

**Swift Developer**

Details 38 Courses, 20 Hours, 24 CPE Credits
Core

Designed to provide an understanding of security principles, best practices for developing secure mobile applications, and essential access control on mobile devices. The Learning Path also focuses on fundamentals of application security, application security risk management, and common vulnerabilities in mobile applications.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 110 Fundamentals of Secure Mobile Development
- ENG 112 Essential Access Control for Mobile Devices
- ENG 205 Fundamentals of Threat Modeling

Advanced

Explains how to identify common mobile application risks and utilize best practices for designing and building applications for iOS and OS ZX. Covers key fundamentals of mobile application threats and mitigations, mobile data cryptograph to provide a solid foundation for creating secure code for swift applications. This path also covers Mobile OWASP Top 10, to educate learners about the consequences of the most common and most important application security weaknesses to enable the learner to develop secure code and mitigate security vulnerabilities.

**Courses Include**

- COD 229 Insecure IoT Mobile Interface
- **COD 234-237 Mobile OWASP Top 10 Series (4)**
- COD 317 Creating Secure iOS Code in Swift
- **DES 202-205 Fundamentals of Cryptography Series (4)**
- TST 252 Testing for OS Command Injection
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 270 Testing for Incorrect Calculation of Buffer Size
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling using the Microsoft Security Development Lifecycle (SDL) process. Developers 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, and guidelines for source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- **ENG 191-195 Integrating the MS SDL into your SDLC Series** (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

**Microsoft SDL**  
**Details** 28 Courses, 17 Hours, 20 CPE Credits

**Core**
Provides a baseline understanding of security principles and best practices for developing secure applications while focusing on fundamentals of application security, application risk management, and common vulnerabilities in an application. This learning path also covers key concepts of cryptography and creating secure code for .NET, MS SQL Applications, and Azure applications.

**Courses Include**
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- **COD 102-108 Fundamentals of SDLC Security Series** (7)
- COD 216-217 Creating Secure .NET Framework Foundations Series (2)
- COD 242 Creating Secure SQL Server & Azure SQL Applications
- COD 254 Creating Secure Azure Applications
- **DES 202-205 Fundamentals of Cryptography Series** (4)

**Elite**
Introduces learner to implementing a holistic and practical approach of the Microsoft Security Development Lifecycle (SDL) and how to apply security and privacy early and throughout all phases of the development process while providing an understanding of secure architecture and design principles. Explores security requirements to be considered during the requirements phase and define the attack surface of an application to reduce the risk to an application and guidelines for secure source code review.

**Courses Include**
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- **ENG 191-195 Implementing the MS SDL into your SDLC Series**
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction
- ENG 312 How to Perform a Security Code Review

**Cloud Developer**  
**Details** 45 Courses, 24 Hours, 29 CPE Credits

**Core**
Designed to provide an understanding of security principles and best practices for developing secure cloud applications with a focus on fundamentals of application security, application security risk management, and common vulnerabilities in an application.

**Courses Include**
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 152 Fundamentals of Secure Cloud Development
- COD 261 Threats to Scripts
- ENG 205 Fundamentals of Threat Modeling

**Advanced**

Examines security vulnerabilities, threats, and mitigations for AWS, Azure cloud computing services and Web APIs covering key concepts of cryptography and the OWASP Top 10 Threats and Mitigations. Cloud developers are educated about the consequences of the most common and most important application security weaknesses to enable developers to develop secure code and mitigate security vulnerabilities.

**Courses Include**

- COD 225-230 IoT Specialization Series (6)
- COD 241 Creating Secure Oracle Database Applications
- COD 253 Creating Secure Creating Secure AWS Cloud Applications
- COD 254 Creating Secure Azure Applications
- COD 255 Creating Secure Code – Web API Foundations
- COD 259 Node.js Threats and Vulnerabilities
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 214-216 Secure Enterprise Infrastructure Series (3)
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction
- ENG 312 How to Perform a Security Code Review

**PCI Developer**

**Details** 67 Courses, 27 Hours, 32 CPE Credits

**Core**

Provides an understand of security principles and best practices for developing secure applications and secure database. Courses focus on fundamentals of application security, application security risk management, common vulnerabilities in an application, and threat modeling.

**Courses Include**

- AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• COD 102-108 Fundamentals of SDLC Security Series (7)
• COD 141 Fundamentals of Secure Database Development
• COD 152 Fundamentals of Secure Cloud Development
• COD 153 Fundamentals of Secure AJAX Code
• ENG 205 Fundamentals of Threat Modeling

Advanced

Provides learners with the tools required to meet the Payment Card Industry Data Security Standards (PCI DSS) for systems that transmit, process, and/or store cardholder data. Courses provide a framework for developing secure applications, explain testing procedures and provide guidance for mitigating OWASP Top 10 and the consequences of CWE’s most dangerous software errors while diving into basic concepts of cryptography and common ways that it is applied, from the perspective of application development while learning to test for vulnerabilities and mitigate security vulnerabilities.

Courses Include

• COD 225-230 IoT Specialization Series (6)
• COD 241 Creating Secure Oracle Database Applications
• COD 246-249 PCI Compliance for Developers Series (4)
• DES 202-205 Fundamentals of Cryptography Series (4)
• DES 214-216 Secure Enterprise Infrastructure Series (3)
• DES 222-231 Applying OWASP 2017 Mitigations Series (10)
• TST 253 Testing for Classic Buffer Overflow
• TST 256 Testing for Missing Authorization
• TST 257 Testing for Use of Hard-Coded Credentials
• TST 258 Testing for Missing Encryption of Sensitive Data
• TST 259 Testing for Unrestricted Upload of File with Dangerous Type
• TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
• TST 261 Testing for Execution with Unnecessary Privileges
• TST 262 Testing for Cross-Site Request Forgery
• TST 264 Testing for Download of Code without Integrity Check
• TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
• TST 267 Testing for Incorrect Permission Assignment for Critical Resource
• TST 268 Testing for Use of a Potentially Dangerous Function
• TST 269 Testing for Use of a Broken or Risky Cryptographic Algorithm
• TST 272 Testing for Open Redirect
• TST 273 Testing for Uncontrolled Format String

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learners to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

• DES 101 Fundamentals of Secure Architecture
• DES 212 Architecture Risk Analysis and Remediation
• ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
• ENG 211 How to Create Application Security Design Requirements
Embedded Developer

Details 34 Courses, 18 Hours, 21 CPE Credits

Core

Provides an understanding of security principles and best practices for developing secure embedded applications. Course focus on fundamentals of application security, application security risk management, common vulnerabilities in an application, and threat modeling.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 110 Fundamentals of Secure Mobile Development
- COD 160 Fundamentals of Secure Embedded Software Development
- COD 261 Threats to Scripts
- DES 260 Fundamentals of IoT Architecture and Design
- ENG 205 Fundamentals of Threat Modeling

Advanced

Provides an understanding of key concepts for common C vulnerabilities and attacks, protecting data in C++, and IoT embedded systems. Covers basic concepts of cryptography and common ways that it is applied from the perspective of application development.

Courses Include

- COD 201-202 Creating Secure C Code Series (2)
- COD 225-230 IoT Specialization Series (6)
- COD 206-207, 307 Creating
- COD 301-303 Protecting C Code Series
- DES 202-205 Fundamentals of Cryptography Series (4)

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- ENG 191-195 Implementing the MS SDL into your SDLC (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction
- ENG 312 How to Perform a Security Code Review
Core Developer

Details 48 Courses, 21 Hours, 25 CPE Credits

Core

Provides an understand of security principles and best practices for developing secure applications and secure database. Coursers focus on fundamentals of application security, application security risk management, common vulnerabilities in an application, and threat modeling to help identify security design problems early in the application security design process.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 102-108 Fundamentals of SDLC Security Series (7)
- COD 141 Fundamentals of Secure Database Development
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers basic concepts of cryptography and common ways that it is applied from the perspective of application development. Architects are also educated on OWASP Top 10 and the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks. Learners will also learn to identify and mitigate CWE’s Top 25 Software errors and enables them to provide recommendations to mitigate these security vulnerabilities.

Courses Include

- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)
- TST 255 Testing for Missing Authentication for Critical Function
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect
- TST 273 Testing for Uncontrolled Format String

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
• DES 212 Architecture Risk Analysis and Remediation
• ENG 191-195 Implementing the MS SDL into your SDLC (5)
• ENG 211 How to Create Application Security Design Requirements
• ENG 311 Attack Surface Analysis and Reduction
• ENG 312 How to Perform a Security Code Review

DevOps Engineer

Details 22 Courses, 9 Hours, 11 CPE Credits

Provides learners with a solid foundation of security features necessary to automate and streamline operations and processes while keeping security top of mind. Learners will apply best practices to develop new features and write scripts across various technologies.

Courses Include

• COD 102-108 Fundamentals of SDLC Security Series (7)
• DES 101 Fundamentals of Secure Architecture
• DES 214-216 Secure Enterprise Infrastructure Series (3)
• ENG 123 Essential Security Engineering Principles
• ENG 124 Essential Application Protection
• ENG 125 Essential Data Protection
• ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
• ENG 205 Fundamentals of Threat Modeling
• TST 101 Fundamentals of Security Testing
• ENG 312 How to Perform a Security Code Review

Network Engineer

Details 25 Courses, 10 Hours, 12 CPE Credits

Provides best practices for managing systems and services across all environments while diving into how to improve the stability, security, efficiency, and scalability of environments. Learners will also develop working knowledge of how to create and modify scripts or applications to perform tasks.

Courses Include

• AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• COD 110 Fundamentals of Secure Mobile Development
• ENG 110 Essential Account Management Security
• ENG 114 Essential Risk Assessment
• ENG 115 Essential System and Information Integrity
• ENG 119 Essential Security Audit and Accountability
• ENG 121 Essential Identification and Authentication
• ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
• TST 101 Fundamentals of Security Testing
• COD 261-266 Secure Scripting Series (4)
• DES 214-216 Secure Enterprise Infrastructure Series (3)
• DES 260 Fundamentals of IoT Architecture and Design
• ENG 205 Fundamentals of Threat Modeling
Automation Engineer

**Details 36 Courses, 9 Hours, 10 CPE Credits**

Introduces learners to essential goals and controls needed to create secure software and manage risk in the software development lifecycle. Courses will also expose learners to cryptography, handling input and output and the and the consequences of the most common and most important application security weaknesses and mitigation of security vulnerabilities using common standards and frameworks.

**Courses Include**

- ENG 110 Essential Account Management Security
- ENG 113 Essential Secure Configuration Management
- ENG 114 Essential Risk Assessment
- ENG 119 Essential Security Audit and Accountability
- ENG 120 Essential Assessment and Authorization
- ENG 123 Essential Security Engineering Principles
- ENG 124 Essential Application Protection
- ENG 125 Essential Data Protection
- DES 222-231 Applying OWASP 2017 Mitigations Series *(10)*
- TST 252 Testing for OS Command Injection
- TST 253 Testing for Classic Buffer Overflow
- TST 255 Testing for Missing Authentication for Critical Function
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 258 Testing for Missing Encryption of Sensitive Data
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 269 Testing for Use of a Broken or Risky Cryptographic Algorithm
- TST 270 Testing for Incorrect Calculation of Buffer Size
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect
- TST 273 Testing for Uncontrolled Format String
- TST 275 Testing for Use of a One-Way Hash without a Salt

Embedded QA/Test Engineer

**Details 41 Courses, 14 Hours, 17 CPE Credits**

**Core**

Provides learners with an understanding of security principles and best practices for developing secure applications and secure database with a focus on fundamentals of application security, application security risk management, common vulnerabilities in an application. Introduces security-testing concepts and processes that will help Embedded QA/Test Engineers analyze an application from a security perspective to conduct effective security testing.

**Courses Include**

- AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• DES 260 Fundamentals of IoT Architecture and Design
• ENG 114 Essential Risk Assessment
• ENG 123 Essential Security Engineering Principles
• ENG 205 Fundamentals of Threat Modeling
• TST 101 Fundamentals of Security Testing

**Advanced**

Provides a solid understanding of how to identify and mitigate each of the and how to test for OWASP 2017 vulnerabilities as well has how to identify and mitigate threats. Engineers will be educated on OWASP Top 10 and the consequences of CWE’s most dangerous software errors to enable development teams to develop secure code and mitigate security vulnerabilities using common standards and frameworks. Dives into basic concepts of cryptography and common ways that it is applied, from the perspective of application development while learning to test for vulnerabilities and provide recommendations to mitigate security vulnerabilities.

*Courses Include*

- TST 222-231 Testing for OWASP Top 10 Series *(10)*
- TST 253 Testing for Classic Buffer Overflow
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 258 Testing for Missing Encryption of Sensitive Data
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 262 Testing for Cross-Site Request Forgery
- TST 264 Testing for Download of Code Without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 270 Testing for Incorrect Calculation of Buffer Size
- TST 273 Testing for Uncontrolled Format String
- TST 274 Testing for Integer Overflow or Wraparound
- TST 275 Testing for Use of One-Way Hash Without A Salt

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

*Courses Include*

- ENG 191-195 Implementing the MS SDLC into your SDLC Series *(10)*
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction
- ENG 312 How to Perform a Security Code Review

**Quality Assurance (QA)/Test Engineer**

*Details* 60 Courses, 19 Hours, 22 CPE Credits

www.securityinnovation.com | @SecInnovation | 978.694.1008
Provides learners with an understanding of security principles and best practices for developing secure applications and secure database with a focus on fundamentals of application security, application security risk management, common vulnerabilities in an application. Introduces security-testing concepts and processes that will help QA/Test Engineers analyze an application from a security perspective to conduct effective security testing.

**Courses Include**
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- ENG 114 Essential Risk Assessment
- ENG 123 Essential Security Engineering Principles
- ENG 205 Fundamentals of Threat Modeling
- TST 101 Fundamentals of Security Testing

**Advanced**
Provides a solid understanding of how to identify and mitigate each of the CWE’s most dangerous software errors and how to test for OWASP 2017 vulnerabilities as well has how to identify and mitigate threats. Dives into basic concepts of cryptography and common ways that it is applied, from the perspective of application development while learning to test for vulnerabilities and provide recommendations to mitigate security vulnerabilities.

**Courses Include**
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 214-216 Secure Enterprise Infrastructure Series (3)
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)
- TST 222-231 Testing for OWASP 2017 Series (10)
- TST 251-275 Testing for CWE SANS Top Software Errors Series (25)

**Elite**
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**
- ENG 211 How to Create Application Security Design Requirements
- ENG 312 How to Perform a Security Code Review

**IT Architect**
**Details** 17 Courses, 11 Hours, 13 CPE Credits
Provides learners with best practices for the design of secure software and how to apply best practices to the creation of integrated architecture across business and technology and protect data and resources from disclosure, modification and deletion.

**Courses Include**
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- DES 260 Fundamentals of IoT Architecture and Design
- COD 253 Creating Secure AWS Cloud Applications
- DES 214-216 Secure Enterprise Infrastructure Series (3)
- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction

**Embedded Architect**

**Details** 11 Courses, 8 Hours, 10 CPE Credits

Provides learners with best practices for the design of secure software for embedded devices systems. Learners will explore the unique resource requirements of embedded environments and best practices for the design and architecting of secure software for embedded systems.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 260 Fundamentals of IoT Architecture and Design
- DES 311 Creating Secure Application Architecture
- **ENG 191-195 Implementing the MS SDL into your SDLC Series (5)**
- ENG 311 Attack Surface Analysis and Reduction
- ENG 312 How to Perform a Security Code Review

**Software Architect**

**Details** 53 Courses, 22 Hours, 26 CPE Credits

**Core**

Provides learners with an understanding of security principles and best practices for developing secure applications, secure database, secure cloud applications, and secure configuration management. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- **COD 102-108 Fundamentals of SDLC Security Series (7)**
- COD 141 Fundamentals of Secure Database Development
- COD 261 Threats to Scripts
- DES 260 Fundamentals of IoT Architecture and Design

**Advanced**

Covers basic concepts of cryptography and common ways that it is applied from the perspective of application development. Architects are also educated on OWASP Top 10 and the consequences of the most common and most important application security weaknesses to enable the developer to develop secure code and mitigate security vulnerabilities using common standards and frameworks. Learners will also learn to identify and mitigate CWE’s Top 25 Software errors and enables them to provide recommendations to mitigate these security vulnerabilities.
Courses Include

- COD 225-230 IoT Specialization Series (6)
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 214-216 Secure Enterprise Infrastructure Series (3)
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)
- TST 255 Testing for Missing Authentication for Critical Function
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
- TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
- TST 267 Testing for Incorrect Permission Assignment for Critical Resource
- TST 268 Testing for Use of a Potentially Dangerous Function
- TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
- TST 272 Testing for Open Redirect
- TST 273 Testing for Uncontrolled Format String

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 101 Fundamentals of Secure Architecture
- DES 212 Architecture Risk Analysis and Remediation
- DES 311 Creating Secure Application Architecture
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis & Reduction
- ENG 312 How to Perform a Security Code Review

Business Analyst

Details 7 Courses, 4 Hours, 5 CPE Credits

Provides learners with the knowledge and skills necessary to ensure adherence to system and information security policies as well as compliance with relevant governmental and industry standards. This learning path also introduces learners to the essentials of access control, configuration management, risk assessment, auditing and authentication.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- DES 101 Fundamentals of Secure Architecture
- ENG 114 Essential Risk Assessment
- ENG 116 Essentials Security Planning Policy and Procedures
- ENG 117 Essential Information Security Program Planning
- ENG 211 How to Create Application Security Design Requirements
Systems Analyst

**Details 37 Courses, 11 Hours, 13 CPE Credits**

Provides fundamental knowledge required to secure networks and systems. Designed to present a holistic approach to network and system security with an exploration of controls, monitoring access, operational procedure and formal auditing and logging.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- ENG 110 Essential Account Management Security
- ENG 111 Essential Session Management Security
- ENG 112 Essential Access Control for Mobile Devices
- ENG 113 Essential Secure Configuration Management
- ENG 114 Essential Risk Assessment
- ENG 115 Essential System and Information Integrity
- ENG 116 Essential Security Planning Policy and Procedures
- ENG 117 Essential Information Security Program Planning
- ENG 118 Essential Incident Response
- ENG 119 Essential Security Audit and Accountability
- ENG 120 Essential Security Assessment and Authorization
- ENG 121 Essential Identification and Authentication
- ENG 122 Essential Physical and Environmental Protection
- ENG 123 Essential Security Engineering Principles
- ENG 124 Essential Application Protection
- ENG 125 Essential Data Protection
- ENG 126 Essential Security Maintenance Policies
- ENG 127 Essential Media Protection
- **ENG 191-195 Implementing the MS SDL into your SDLC Series (5)**
- **DES 222-231 Applying OWASP 2017 Mitigations Series (10)**
- ENG 205 Fundamentals of Threat Modeling
- ENG 211 How to Create Application Security Design Requirements

Systems Administrator

**Details 39 Courses, 15 Hours, 18 CPE Credits**

Provides learners with fundamental knowledge necessary to secure networks and systems. This learning path is designed to present a holistic approach to network and system security with an exploration of controls, monitoring access, operational procedure and formal auditing and logging.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 141 Fundamentals of Secure Database Development
- COD 219 Creating Secure Code SAP ABAP Foundations
- COD 261-266 Secure Scripting Series (4)
- **DES 214-216 Secure Enterprise Infrastructure Series (3)**
- **DES 222-231 Applying OWASP 2017 Mitigations Series (10)**
- ENG 110 Essential Account Management Security
Database Administrator

Details 47 Courses, 25 Hours, 30 CPE Credits

Core

Provides fundamental knowledge of secure database development and the common database attacks that can be used to cause significant loss to an organization while providing learners with an understanding of security principles and best practices for developing secure applications, secure database, secure cloud applications, and secure configuration management. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

Courses Include

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- COD 141 Fundamentals of Secure Database Development
- COD 261 Threats to Scripts
- COD 262 Fundamentals of Shell and Interpreted Language Security
- ENG 205 Fundamentals of Threat Modeling

Advanced

Covers basic concepts of cryptography and common ways that it is applied from the perspective of database development while diving into platform-specific threats and secure coding best practices. Provides a solid understanding of OWASP Top 10 and the consequences of the most common and most important application security weaknesses. Learners will also learn to identify and mitigate CWE’s Top 25 Software errors and enables them to provide recommendations to mitigate these security vulnerabilities.

Courses Include

- COD 241 Creating Secure Code - Oracle Database Applications
- COD 242 Creating Secure SQL Server and Azure SQL Database Applications
- COD 352 Creating Secure jQuery Code
- DES 202-205 Fundamentals of Cryptography Series (4)
- DES 222-231 Applying OWASP 2017 Mitigations Series (10)
- TST 255 Testing for Missing Authentication for Critical Function
- TST 257 Testing for Use of Hard-Coded Credentials
- TST 259 Testing for Unrestricted Upload of File with Dangerous Type
- TST 260 Testing for Reliance on Untrusted Inputs in a Security Decision
- TST 261 Testing for Execution with Unnecessary Privileges
- TST 264 Testing for Download of Code without Integrity Check
• TST 266 Testing for Inclusion of Functionality from Untrusted Control Sphere
• TST 267 Testing for Incorrect Permission Assignment for Critical Resource
• TST 268 Testing for Use of a Potentially Dangerous Function
• TST 271 Testing for Improper Restriction of Excessive Authentication Attempts
• TST 272 Testing for Open Redirect
• TST 273 Testing for Uncontrolled Format String

Elite
Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include
• DES 101 Fundamentals of Secure Architecture
• DES 212 Architecture Risk Analysis and Remediation
• ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
• ENG 211 How to Create Application Security Design Requirements
• ENG 311 Attack Surface Analysis and Reduction
• ENG 312 How to Perform a Security Code Review

Linux Administrator
Details 20 Courses, 7 Hours, 9 CPE Credits
Dives into operating system configuration and administration of virtual servers. Learners will develop working knowledge needed to support development, testing and systems integration. Additionally, the learning path will provide learners with a solid understanding of secure development best practices.

Courses Include
• ENG 110 Essential Account Management Security
• ENG 114 Essential Risk Assessment
• ENG 115 Essential System and Information Integrity
• ENG 119 Essential Security Audit and Accountability
• ENG 121 Essential Identification and Authentication
• COD 261-266 Secure Scripting Series (6)
• ENG 205 Fundamentals of Threat Modeling
• DES 214 Securing Infrastructure Architecture
• DES 215 Defending Infrastructure
• ENG 191-195 Implementing the MS SDL into your SDLC Series (5)

Application/Product Owner
Details 24 Courses, 9 Hours, 11 CPE Credits
Provides those responsible for setting, prioritizing, and evaluating the work generated by a software development by introducing the learner to the basics of application security and essentials goals and controls needed to create secure software and manage risk in the software development lifecycle.

Courses Include

www.securityinnovation.com | @SecInnovation | 978.694.1008
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- DES 260 Fundamentals of IoT Architecture and Design
- ENG 124 Essential Application Protection
- ENG 125 Essential Data Protection
- TST 101 Fundamentals of Security Testing
- **DES 222-231 Applying OWASP 2017 Mitigations Series (10)**
- DES 212 Architecture Risk Analysis and Remediation
- **ENG 191-195 Implementing the MS SDL into your SDLC Series (5)**
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction

**Project Manager**

**Details** 24 Courses, 13 Hours, 15 CPE Credits

**Core**

Provides learners with an understanding of security engineering principles, data protection principles and best practices for developing secure applications. The learning path focuses on fundamentals of application security, application security risk management, common vulnerabilities in an application.

**Courses Include**

- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- **COD 102-108 Fundamentals of SDLC Security Series (7)**
- COD 141 Fundamentals of Secure Database Development*
- COD 152 Fundamentals of Secure Cloud Development*
- ENG 123 Essential Security Engineering Principles
- ENG 124 Essential Applications Protection
- ENG 125 Essential Data Protection
- ENG 205 Fundamentals of Threat Modeling

**Advanced**

Covers basic concepts of cryptography and the common ways to apply cryptography from the perspective of application development. Courses will cover the risks associated with data breaches and how to implement strong access controls and security policies that protect applications, systems, and sensitive data.

**Courses Include**

- **DES 202-205 Fundamentals of Cryptography Series (4)**
- DES 214 Securing Infrastructure Architecture
- DES 215 Defending Infrastructure

**Elite**

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

**Courses Include**

- DES 101 Fundamentals of Secure Architecture
Cyber Security Professional

**Details** 15 Courses, 4 Hours, 5 CPE Credits

Provides learners with fundamental security skills required to develop and design security devices and software. Learners will explore how to manage security measures, operate inspections of systems and process, initiate security and safety measures, and maintain policies and procedures, and information security and privacy best practices.

**Courses Include**

- AWA 008 Information Privacy – Classifying Data
- AWA 009 Information Privacy – Protecting Data
- AWA 010 Email Security
- AWA 012 Malware Awareness
- AWA 013 Mobile Security
- AWA 014 Password Security
- AWA 016 Phishing Awareness
- AWA 018 Social Engineering Awareness
- AWA 019 Travel Security
- AWA 101 Fundamentals of Application Security
- AWA 102 Secure Software Concepts
- ENG 117 Essential Information Security Program Planning
- ENG 118 Essential Incident Response
- ENG 124 Essential Application Protection
- TST 101 Fundamentals of Software Security Testing

Operations/IT Manager

**Details** 22 Courses, 7 Hours, 8 CPE Credits

Introduces basics of application security and essential goals and controls needed to manage the development of secure software. Courses will also explore management of risks associated with the software development lifecycle while diving into developing, implementing, and ensuring compliance with operational application security policies and procedures.

**Courses Include**

- DES 214-216 Secure Enterprise Infrastructure Series (3)
- ENG 110 Essential Account Management Security
- ENG 111 Essential Session Management Security
- ENG 112 Essential Access Control for Mobile Devices
- ENG 113 Essential Secure Configuration Management
- ENG 114 Essential Risk Assessment
- ENG 115 Essential System and Information Integrity
- ENG 116 Essential Security Planning Policy and Procedures
- ENG 117 Essential Information Security Program Planning
- ENG 118 Essential Incident Response
- ENG 119 Essential Security Audit and Accountability
- ENG 120 Essential Security Assessment and Authorization
• ENG 121 Essential Identification and Authentication
• ENG 122 Essential Physical and Environmental Protection
• ENG 123 Essential Security Engineering Principles
• ENG 124 Essential Application Protection
• ENG 125 Essential Data Protection
• ENG 126 Essential Security Maintenance Policies
• ENG 127 Essential Media Protection
• ENG 205 Fundamentals of Threat Modeling

Application Security Champion

Details 30 Courses, 10 Hours, 12 CPE Credits

Exposes learners to concepts around all aspects of security including privacy, secure development and architecture, security testing, threat modeling, cryptography and cyber threat analysis and remediation.

Courses Include

• AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• COD 102-108 Fundamentals of SDLC Security Series (7)
• ENG 124 Essential Application Protection
• ENG 125 Essential Data Protection
• TST 101 Fundamentals of Security Testing
• DES 212 Architecture Risk Analysis and Remediation
• DES 222-231 Applying OWASP 2017 Mitigations Series (10)
• ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
• ENG 211 How to Create Application Security Design Requirements
• ENG 311 Attack Surface Analysis and Reduction

Information Security Specialist

Details 41 Courses, 19 Hours, 23 CPE Credits

Core

Provides an understanding of security principles and best practices for identifying, protecting, detecting, and recovering from risks, vulnerabilities, and threats to the secure of information and/or data.

Courses Include

• AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• COD 141 Fundamentals of Secure Database Development
• COD 261 Threats to Scripts
• ENG 110 Essential Account Management Security
• ENG 111 Essential Session Management Security
• ENG 112 Essential Access Control for Mobile Devices
• ENG 113 Essential Secure Configuration Management
• ENG 114 Essential Risk Assessment
• ENG 115 Essential System and Information Integrity
• ENG 116 Essential Security Planning Policy and Procedures
• ENG 117 Essential Information Security Program Planning
• ENG 118 Essential Incident Response
Advanced

Provides an understanding of how to protect sensitive data ensuring data integrity for applications running on Microsoft SQL server and Oracle database. Courses also provide an in-depth understanding of application security requirements during the design and build stages of the development lifecycle, which significantly facilitates compliance.

Courses Include

- COD 234 Mobile Threats and Mitigations
- COD 241 Creating Secure Code Oracle Foundations
- COD 242 Creating Secure SQL Server & Azure SQL Database Applications
- COD 246-249 PCI Compliance for Developers Series (4)
- COD 256 Creating Secure Code Ruby on Rails Foundations

Elite

Provides learners with an understanding of secure architecture and design principles while articulating security requirements to be considered during the requirements phase. This path also introduces the learner to threat modeling to help identify security design problems early in the application security design process. Developers 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, and guidelines for secure source code review.

Courses Include

- DES 212 Architecture Risk Analysis and Remediation
- ENG 191-195 Implementing the MS SDL into your SDLC Series (5)
- ENG 211 How to Create Application Security Design Requirements
- ENG 311 Attack Surface Analysis and Reduction
- ENG 312 How to Perform a Security Code Review

Systems Leadership

Details 13 Courses, 5 Hours, 6 CPE Credits

Provides learners with a comprehensive baseline of application security knowledge necessary for leading application development and design projects. Courses explore application security best practices necessary to ensure strategies and plans that support business needs and align with departmental and organizational objectives and goals.

Courses Include

- AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• DES 222-231 Applying OWASP 2017 Mitigations Series (10)
• DES 311 Creating Secure Application Architecture

Development Manager

Details 14 Courses, 7 Hours, 8 CPE Credits

Introduces application security best practices required to adhere to system and information security policies and compliance. Learners will learn how to apply these best practices to requirements, design, and implementation phases of the software development lifecycle.

Courses Include

• AWA 101 Fundamentals of Application Security
• AWA 102 Secure Software Concepts
• DES 260 Fundamentals of IoT Architecture and Design
• ENG 110 Essential Account Management Security
• ENG 114 Essential Risk Assessment
• ENG 117 Essential Information Security Program Planning
• ENG 205 Fundamentals of Threat Modeling
• ENG 191-195 Implementing the MS SDLC into your SDLC Series (10)
• DES 101 Fundamentals of Secure Architecture
• ENG 211 How to Create Application Security Design Requirements