LEARNING PATHS

Software Security Role-Based Curriculum

.NET Developer

The .NET learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide a solid foundation of .NET security features for building secure web applications, sophisticated desktop applications, or modern mobile applications. Security concepts covered within this learning path include:

- Code Access Security (CAS)
- .NET cryptographic technologies
- Secure Coding best practices

More advanced courses offer application framework specific secure coding best practices for ASP.NET to extend the .NET Developer platform with tools and libraries for building web applications. Round off security expertise with knowledge and skills to apply security principles for creating secure application architecture and conduct effective security code reviews.

Details 33 Courses, 11 Hours, 14 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 216-217 Creating Secure Code .NET Framework Foundations Series (2) COD 255 Creating Secure Code – Web API Foundations DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigation Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 308-309 Creating Secure ASP.NET MVC Applications Series (2) DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Android Developer

The Android Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide a solid foundation of security features necessary to develop applications for devices powered by the Android operating system. The Android Developer learning path provides secure coding best practices for designing and building android applications including:

- Identifying common android application risks

- Creating a mobile application threat model
- Applying android platform specific knowledge

Round off security expertise with knowledge and skills to apply security principles for creating secure application architecture and conduct effective security code reviews.

Details 43 Courses, 13 Hours, 16 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security	COD 286 Creating Secure React User Interfaces	COD 318 Protecting Data on Android in Java
AWA 102 Secure Software Concepts	DES 204 The Role of Cryptography in Application Development	COD 319 Preventing Vulnerabilities in Android Code using Java
COD 102-108 Fundamentals of SDLC Security Series (7)	DES 212 Architecture Risk Analysis and Remediation	COD 327 Testing for OS Command Injection
DES 101 Fundamentals of Secure Architecture	DES 260 Fundamentals of IoT Architecture and Design	COD 332 Testing for Use of Hard-Coded Credentials
ENG 112 Essential Access Control for Mobile Devices	DES 271-280 Mobile OWASP Top 10 Series (10)	COD 334 Testing for Unrestricted Upload of File with Dangerous Type
	DES 286 OWASP IoT6: Mitigating Insufficient Privacy Protection	COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision
	DES 287 OWASP IoT7: Mitigating Insecure Data Transfer and Storage	COD 336 Testing for Execution with Unnecessary Privileges
	DES 289 OWASP IoT9: Mitigating Insecure Default Settings	COD 339 Testing for Download of Code without Integrity Check
	ENG 205 Fundamentals of Threat Modeling	COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere
	COD 286 Creating Secure React User Interfaces	COD 342 Testing for Incorrect Permission Assignment for Critical Resource
	DES 287 OWASP IoT7: Mitigating Insecure Data Transfer and Storage	COD 343 Testing for Use of a Potentially Dangerous Function
	DES 289 OWASP IoT9: Mitigating Insecure Default Settings	COD 345 Testing for Incorrect Calculation of Buffer Size
	ENG 205 Fundamentals of Threat Modeling	COD 346 Testing for Improper Restriction of Excessive Authentication Attempts
	ENG 211 How to Create Application Security Design Requirements	COD 347 Testing for Open Redirect
	ENG 212 Implementing Secure Software Operations	COD 366 Creating Secure Kotlin Applications
		DES 311 Creating Secure Application Architecture
		DSO 307 Secure Secrets Management
		ENG 312 How to Perform a Security Code Review

Back-End Developer

The Back-end Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide a solid foundation of security features needed to write web services and API's used by front-end and mobile application developers. The Back-end Developer learning path presents secure coding best practices in all phases of the development life cycle across cutting-edge technologies like Node.js, Angular.js, and MySQL with special attention to managing the interchange of data between the server and users.

Details 30 Courses, 11 Hours, 13 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security	COD 241 Creating Secure Oracle Database Applications	COD 352 Creating Secure JavaScript and jQuery Code
AWA 102 Secure Software Concepts	COD 251 Defending AJAX-enabled Web Applications	COD 372 Testing for OWASP 2017 Sensitive Data Exposure
COD 102-108 Fundamentals of SDLC Security Series (7)	COD 255 Creating Secure Code – Web API Foundations	COD 375 Testing for OWASP 2017 Security Misconfiguration
DES 101 Fundamentals of Secure Architecture	COD 267 Securing Python Microservices	COD 383 Protecting Java Backend Services
	COD 287 Java Application Server Hardening	DES 311 Creating Secure Application Architecture
	DES 204 The Role of Cryptography in Application Development	DSO 304 Securing API Gateways in a DevSecOps Framework
	DES 212 Architecture Risk Analysis and Remediation	DSO 307 Secure Secrets Management
	DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure	ENG 312 How to Perform a Security Code Review
	DES 227 Applying OWASP 2017 Mitigating Security Misconfiguration	
	ENG 205 Fundamentals of Threat Modeling	
	ENG 211 How to Create Application Security Design Requirements.	
	ENG 212 Implementing Secure Software Operations	

C Developer

The C Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide a solid understanding of security features required to develop secure code that integrates into operating systems, operating system modules, embedded systems, or low-level libraries for other high-level languages. The C Developer learning path covers key application security concepts including:

- Memory management and string handling
- Avoiding common pitfalls
- C specific security flaws

Details 36 Courses, 12 Hours, 14 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 201-202 Creating Secure C Code Series (2) COD 261 Threats to Scripts DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 301-303 Protecting C Code Series (3) COD 330 Testing for Missing Authentication for Critical Function COD 332 Testing for use of Hard-Coded Credentials COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance of Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges COD 339 Testing for Download of Code without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

C# Developer

The C# Developer Learning Path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It builds a thorough grounding of security features necessary to develop modern applications that run on desktops or back-end processes powering modern web applications. The C# Developer learning path covers key application security concepts including:

- Defensive coding best practices
- Developing scalable applications using multithreading features of .NET framework
- Avoiding common pitfalls

Details 36 Courses, 12 Hours, 15 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security	COD 216-217 Creating Secure Code .NET Framework Foundations Series (2)	COD 308-309 Creating Secure ASP.NET MVC Applications Series (2)
AWA 102 Secure Software Concepts	DES 204 The Role of Cryptography in Application Development	COD 321-324 Protecting C# Series (4)
COD 102-108 Fundamentals of SDLC Security Series (7)	DES 212 Architecture Risk Analysis and Remediation	DES 311 Creating Secure Application Architecture
DES 101 Fundamentals of Secure Architecture	DES 281-290 OWASP IoT Top 10 Series (10)	DSO 307 Secure Secrets Management
	ENG 205 Fundamentals of Threat Modeling	ENG 312 How to Perform a Security Code Review
	ENG 211 How to Create Application Security Design Requirements	
	ENG 212 Implementing Secure Software Operations	

C++ Developer

The C++ Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide a continuous working knowledge of application security best practices for building applications that range from desktop applications to native mobile applications and embedded systems. It also provides the knowledge needed to build efficient, reusable, and reliable C++ code that interacts with low-level systems and hardware resources. Learners will develop the knowledge and skills required to:

- Mitigate memory corruption vulnerabilities
- Protect data in transit using strong TLS ciphers
- Protect data using cryptographic best practices while applying secure coding best practices

Details 40 Courses, 13 Hours, 15 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security	COD 206 Creating Secure C++ Code	COD 307 Protecting Data in C++
AWA 102 Secure Software Concepts	COD 207 Communication Security in C++	COD 330 Testing for Missing Authentication for Critical Function
COD 102-108 Fundamentals of SDLC Security Series (7)	COD 255 Creating Secure Code – Web API Foundations	COD 332 Testing for Use of Hard-Coded Credentials
DES 101 Fundamentals of Secure Architecture	COD 262 Fundamentals of Shell and Interpreted Language Security	COD 334 Testing for Unrestricted Upload of File with Dangerous Type
	COD 263 Secure Bash Scripting	COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision
	COD 264 Secure Perl Scripting	COD 336 Testing for Execution with Unnecessary Privileges
	COD 265 Secure Python Scripting	COD 339 Testing for Download of Code Without Integrity Check
	COD 266 Secure Ruby Scripting	COD 341 Testing for Inclusion of

		Functionality from Untrusted Control Sphere
	DES 203 Cryptographic Components: Randomness, Algorithms, and Key Management DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Front-End Developer

The Front-end Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It provides a solid foundation for using markup languages, design and client-side scripts and framework to create secure environments for everything that users touch. The Front-End Developer learning path covers key application security concepts including:

- Deep dive on HTML, CSS and responsive web development
- How vulnerabilities are discovered and exploited
- How to build a strong line of defense

Details 42 Courses, 15 Hours, 19 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 214 Creating Secure Go Applications COD 251 Defending AJAX-enabled Web Applications COD 255 Creating Secure Code – Web API Foundations COD 256 Creating Secure Code – Ruby on Rails COD 258 Creating Secure PHP Web Applications COD 259 Node.js Threats and Vulnerabilities COD 285 Developing Secure Angular Applications COD 286 Creating Secure React User	COD 352 Creating Secure jQuery Code COD 361-364 Creating Secure HTML5 Code Series (4) DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

	Interfaces DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigations Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	

HTML5 Developer

The HTML5 Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide front-end developers responsible for holding the style and interactivity backbone together with a deeper understanding of HTML5 – and building a strong line of defense. The HTML5 Developer learning path covers key application security concepts including:

- HTML5 security features
- How to infuse software security into the development lifecycle
- Working knowledge of ASP.net, SWL, high-level scripting languages, version control and CMS systems

Details 36 Courses, 14 Hours, 17 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 251 Defending AJAX-enabled Web 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 Java Security Model COD 285 Developing Secure Angular Applications DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure DES 228 Applying OWASP 2017 Mitigating Cross-Site Scripting	COD 308-309 Creating Secure ASP.NET MVC Applications Series (2) COD 352 Creating Secure jQuery Code COD 361-364 Creating Secure HTML5 Code Series (4) COD 372 Testing for OWASP 2017 Sensitive Data Exposure COD 376 Testing for OWASP 2017 Cross-Site Scripting DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

	ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	

iOS Developer

The iOS Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide developers with a solid foundation of security features necessary to develop applications for devices powered by the iOS platform. The iOS Developer learning path provides secure coding best practices for designing and building iOS applications including:

- Identifying common iOS application risks
- Creating a mobile application threat model
- Applying iOS platform-specific knowledge

Details 43 Courses, 13 Hours, 16 CPE Credits

Core	***Advanced***	***Elite***
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 DES 101 Fundamentals of Secure Architecture	COD 286 Creating Secure React User Interfaces DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 260 Fundamentals of IoT Architecture and Design DES 271-280 Mobile OWASP Top 10 Series (10) DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage DES 289 – OWASP IoT9: Mitigating Insecure Default Settings ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 315 Preventing Vulnerabilities in iOS Code using Swift COD 316 Creating Secure iOS Code in Objective C COD 317 Protecting Data on iOS Code in Swift COD 327 Testing for OS Command Injection COD 332 Testing for Use of Hard-Coded Credentials COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges COD 339 Testing for Download of Code without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 345 Testing for Incorrect Calculation of Buffer Size

		COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Java Developer

The Java Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced, or elite paths. It is designed to provide a working knowledge for developing solid and secure Java applications as well as recognizing and remediating common Java web software security vulnerabilities. The Java Developer learning path covers key application security concepts including:

- Java, JRE, and J2EE constructs
- Core implementation practices
- Best practices for designing, developing, and testing Java based solutions using common standards and frameworks

Details 58 Courses, 19 Hours, 23 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 219 Creating Secure Code – SAP ABAP Foundations COD 251 Defending AJAX-enabled Web Applications 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 287 Java Application Server Hardening DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigations Series (10) DES 281-290 OWASP IoT Top 10 Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements	COD 352 Creating Secure JavaScript and jQuery Code COD 361-364 Creating Secure HTML5 Code Series (4) COD 380-386 Protecting Java Code Series (7) DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

	ENG 212 Implementing Secure Software Operations	

JavaScript Developer

The JavaScript Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is intended for those responsible for implementing the front-end logic that defines the behavior of the visual elements of a web application and connecting this with services that may reside on the back-end. The JavaScript Developer learning provides a thorough grounding in application security concepts and implementation practices including:

- JavaScript security flaws
- Proven techniques to help protect JavaScript
- Avoiding common pitfalls

Details 41 Courses, 17 Hours, 20 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 241 Creating Secure Oracle Database Applications COD 251 Defending AJAX-enabled Web Applications COD 255 Creating Secure Code – Web API Foundations COD 256 Creating Secure Code – Ruby on Rails COD 258 Creating Secure PHP Web Applications COD 259 Node.js Threats and Vulnerabilities COD 281-284 Creating Secure Java Code Series (3) COD 285 Developing Secure Angular Applications COD 286 Creating Secure React User Interfaces DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation 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 ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements	COD 352 Creating Secure jQuery Code COD 361-364 Creating Secure HTML5 Code Series (4) COD 372 Testing for OWASP 2017 Sensitive Data Exposure COD 373 Testing for OWASP 2017 XML External Entities COD 376 Testing for OWASP 2017 Cross-Site Scripting DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

	ENG 212 Implementing Secure Software Operations	

Mobile Developer

The Mobile Developer learning path includes a variety of courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide developers with a solid foundation of security features necessary to develop applications for mobile devices. The Mobile Developer learning path covers key application security concepts including:

- Identifying common mobile application risks
- Best practices for designing secure mobile applications
- Coding mistakes to avoid

Details 56 Courses, 17 Hours, 21 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security	COD 261 Threats to Scripts	COD 315 Preventing Vulnerabilities in iOS Code using Swift
AWA 102 Secure Software Concepts	COD 286 Creating Secure React User Interfaces	COD 316 Creating Secure iOS Code in Objective C
COD 110 Fundamentals of Secure Mobile Development	DES 204 The Role of Cryptography in Application Development	COD 317 Protecting Data on iOS in Swift
DES 101 Fundamentals of Secure Architecture	DES 212 Architecture Risk Analysis and Remediation	COD 318 Protecting Data on Android in Java
ENG 112 Essential Access Control for Mobile Devices	DES 255 Securing the IoT Update Process	COD 319 Preventing Vulnerabilities in Android
	DES 260 Fundamentals of IoT Architecture and Design	COD 327 Testing for OS Command Injection
	DES 271-280 Mobile OWASP Top 10 Series (10)	COD 328 Testing for Classic Buffer Overflow
	DES 284 – OWASP IoT4: Mitigating Lack of Secure Update Mechanism	COD 330 Testing for Missing Authorization
	DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection	COD 332 Testing for Use of Hard-Coded Credentials
	DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage	COD 333 Testing for Missing Encryption of Sensitive Data
	DES 288 – OWASP IoT8: Mitigating Lack of Device Management	COD 334 Testing for Unrestricted Upload of File with Dangerous Type
	DES 289 – OWASP IoT9: Mitigating Insecure Default Settings	COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision
	ENG 205 Fundamentals of Threat Modeling	COD 336 Testing for Execution with Unnecessary Privileges
	ENG 211 How to Create Application Security Design Requirements	COD 339 Testing for Download of Code without Integrity Check
	ENG 212 Implementing Secure Software Operations	COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere
		COD 342 Testing for Incorrect Permission Assignment for Critical

		Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 344 Testing for Use of Broken or Risky Cryptographic Algorithm COD 345 Testing for Incorrect Calculation of Buffer Size COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String COD 350 Testing for Use of a One-Way Hash without a Salt COD 366 Creating Secure Kotlin Applications DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

PHP Developer

The PHP learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide PHP developers with a solid foundation of security features necessary to develop server-side web application logic. The PHP learning path offers secure coding best practices to develop back-end web services connection components and support front-end, developers. Learners will be able to apply these security best practices to the entire web application development life cycle from concept stage to delivery and post-launch.

Details 58 Courses, 18 Hours, 22 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 251 Defending AJAX-enabled Web Applications COD 255 Creating Secure Code – Web API Foundations COD 256 Creating Secure Code – Ruby on Rails COD 258 Creating Secure PHP Web Applications COD 259 Node.js Threats and Vulnerabilities COD 261-266 Secure Scripting Series (6)	COD 361-364 Creating Secure HTML5 Code Series (4) COD 370-379 Testing for OWASP 2017 Series (10) DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

	COD 281-284 Creating Secure Java Code Series (4) DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigations Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	

Python Developer

The Python Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for the programming and development of web applications or applications that are run over HTTP from a web server to a web browser. The Python Web Developer learning path covers key application security concepts including:

- Secure coding best practices
- Effective platform configuration
- How to identify and mitigate vulnerabilities

Details 42 Courses, 15 Hours, 18 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 251 Defending AJAX-enabled Web Applications COD 255 Creating Secure Code – Web API Foundations COD 256 Creating Secure Code – Ruby on Rails COD 257 Creating Secure Python Web Applications COD 261 Threats to Scripts COD 262 Fundamentals of Shell and Interpreted Language Security COD 265 Secure Python Scripting COD 267 Securing Python Microservices DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigations Series (10)	COD 361-364 Creating Secure HTML5 Code Series (4) DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 306 Implementing Infrastructure as Code DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

	ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	

Ruby on Rails Developer

The Ruby on Rails learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. This path is designed for those responsible for writing server-side web application logic in Ruby, around the frame rails. It provides best practices and techniques for secure application development, including:

- Understanding various classes of vulnerabilities
- Building strong session management
- Preventing vulnerabilities commonly found in Rails applications

Details 38 Courses, 15 Hours, 18 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 251 Defending AJAX-enabled Web 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 281-284 Creating Secure Java Code Series (3) COD 287 Java Application Server Hardening DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 224 Applying OWASP 2017 Mitigating Sensitive Data Exposure DES 228 Applying OWASP 2017 Mitigating Cross-Site Scripting ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 352 Creating Secure jQuery Code COD 361-364 Creating Secure HTML5 Foundations Series (2) COD 372 Testing for OWASP 2017 Sensitive Data Exposure COD 376 Testing for OWASP 2017 Cross-Site Scripting DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 306 Implementing Infrastructure as Code DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Web Developer

The Web Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for the development of web applications or applications that are run over HTTP from a web server to a web browser. The Web Developer Learning Path provides developers with a solid foundation of security features necessary to develop applications including:

- Responsive web design
- Enterprise integration
- How to protect data with security best practices

Details 54 Courses, 19 Hours, 23 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 241 Creating Secure Oracle Database Applications COD 251 Defending AJAX-enabled Web 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 258 Creating Secure PHP Web Applications COD 259 Node.js Threats and Vulnerabilities COD 261 Threats to Scripts COD 262 Fundamentals of Shell and Interpreted Language Security COD 285 Developing Secure Angular Applications DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigations Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 352 Creating Secure jQuery Code COD 361-364 Creating Secure HTML5 Foundations Series (2) COD 370-379 Testing for OWASP 2017 Mitigations Series (10) DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Node.js Developer

The Node.js learning path includes a variety of security courses that vary depending on whether you are seeking core, advanced or elite paths. It is designed for those that managing the interchange of

data between the server and the users and provides developers a solid foundation of security features necessary to code, test and operate including:

- Node.js based services
- Web libraries, frameworks and the whole web stack
- Protecting data using secure coding best practices

Details 40 Courses, 16 Hours, 19 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture	COD 241 Creating Secure Oracle Database Applications COD 251 Defending AJAX-enabled Web 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 258 Creating Secure PHP Web Applications COD 259 Node.js Threats and Vulnerabilities COD 285 Developing Secure Angular Applications DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation 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 ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 308-309 Creating Secure ASP.NET MVC Applications Series (2) COD 352 Creating Secure jQuery Code COD 361-364 Creating Secure HTML5 Foundations Series (2) COD 372 Testing for OWASP 2017 Sensitive Data Exposure COD 373 Testing for OWASP 2017 XML External Entities COD 376 Testing for OWASP 2017 Cross-Site Scripting DES 311 Creating Secure Application Architecture DSO 304 Securing API Gateways in a DevSecOps Framework DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Swift Developer

The Swift Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. This path is designed for those responsible for the development of applications aimed towards iOS and OS X and the integration with back-end services. The Swift Developer learning path covers key application security concepts including:

- How identify common mobile application risks

- Utilize best practices for designing and building applications for iOS and OS X
- RESTful API's, embedded databases, and object-oriented programming

Details 40 Courses, 12 Hours, 15 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 110 Fundamentals of Secure Mobile Development DES 101 Fundamentals of Secure Architecture ENG 112 Essential Access Control for Mobile Devices	DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 271-280 Mobile OWASP Top 10 Series (10) DES 286 – OWASP IoT6: Mitigating Insufficient Privacy Protection DES 287 – OWASP IoT7: Mitigating Insecure Data Transfer and Storage DES 289 – OWASP IoT9: Mitigating Insecure Default Settings ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 315 Preventing Vulnerabilities in iOS Code using Swift *COD* 317 Protecting Data on iOS in Swift COD 327 Testing for OS Command Injection COD 332 Testing for Use of Hard-Coded Credentials COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges COD 339 Testing for Download of Code without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 345 Testing for Incorrect Calculation of Buffer Size COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Microsoft SDL Developer

The MS SDL Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for implementing the industry-leading software security assurance process. The MS SDL Developer learning path describes how to take a holistic and practical approach when implementing the SDL to

ensure security and privacy is considered at every phase of development.

Details 26 Courses, 10 Hours, 12 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) DES 101 Fundamentals of Secure Architecture ENG 191-195 Implementing the MS SDL into your SDLC Series (5)	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 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	DES 311 Creating Secure Application Architecture DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

Cloud Developer

The Cloud Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for the design, development, and deployment of cloud applications and provides learners with a clear understanding of how to mitigate cloud computing risks. learning path covers key application security topics including

- "Big Data" and it introduces security challenges
- Cloud computing characteristics, service and deployment models, and regulatory requirements
- Platform-specific secure coding best practices including AWS and/or Azure

Details 52 Courses, 19 Hours, 23 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 152 Fundamentals of Secure Cloud Development DES 101 Fundamentals of Secure Architecture	COD 214 Creating Secure Go Applications 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 COD 261 Threats to Scripts COD 267 Securing Python Microservices	DES 311 Creating Secure Application Architecture DSO 301 Orchestrating Secure System & Service Configuration DSO 304 Securing API Gateways in a DevSecOps Framework DSO 305 Automating CI/CD Pipeline Compliance DSO 306 Implementing Infrastructure as Code DSO 307 Secure Secrets Management ENG 311 Attack Surface Analysis and Reduction ENG 312 How to Perform a Security Code Review

	DES 204 The Role of Cryptography in Application Development DES 206 Meeting Cloud Governance and Compliance Requirements DES 212 Architecture Risk Analysis and Remediation DES 214-218 Secure Enterprise Infrastructure Series (4) DES 222-231 Applying OWASP 2017 Mitigations Series (10) DES 281-290 OWASP IoT Top 10 Series (10) DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework DSO 253 DevSecOps in the AWS Cloud DSO 254 DevSecOps in the Azure Cloud ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	

PCI Developer

The PCI learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for developing applications that process credit and debit card payments and/or any type of cardholder data. The PCI Developer learning path 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. The courses within the PCI Developer learning path provide a framework for:

- Developing secure applications
- Conducting effective test procedures
- Adopting guidance for mitigating issues

Details 68 Courses, 21 Hours, 25 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) COD 141 Fundamentals of Database Security	COD 241 Creating Secure Oracle Database Applications COD 246-249 PCI Compliance for Developers Series (4) COD 251 Defending AJAX-enabled Web Applications DES 204 The Role of Cryptography in Application Development	COD 328 Testing for Classic Buffer Overflow COD 331 Testing for Missing Authorization COD 332 Testing for Use of Hard-Coded Credentials COD 333 Testing for Missing Encryption of Sensitive Data

COD 152 Fundamentals of Secure Cloud Development DES 101 Fundamentals of Secure Architecture DES 151 Fundamentals of the PCI Secure SLC Standard	DES 212 Architecture Risk Analysis and Remediation DES 214-218 Secure Enterprise Infrastructure Series (4) DES 222-231 Applying OWASP 2017 Mitigations Series (10) DES 281-290 OWASP IoT Top 10 Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges COD 337 Testing for Cross-Site Request Forgery COD 339 Testing for Download of Code without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 344 Testing for Use of a Broken or Risky Cryptographic Algorithm COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String DES 311 Creating Secure Application Architecture DES 312 Protecting Cardholder Data DSO 307 Secure Secrets Management ENG 311 Attack Surface Analysis and Reduction ENG 312 How to Perform a Security Code Review

IoT & Embedded Developer

The IoT/Embedded learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed to provide developers those responsible for designing and implementing software of embedded devices and systems with the knowledge and skills required to create secure embedded software and devices. The IoT/Embedded learning path provides learners with a thorough grounding in application security concepts across the fundamental courses with special attention to coding within embedded systems and includes secure mobile development.

Details 37 Courses, 14 Hours, 17 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts	COD 201-202 Creating Secure C Code Series (2) COD 206 Creating Secure C++ Code	COD 301-303 Protecting C Code Series (3) COD 307 Protecting Data in C++

COD 110 Fundamentals of Secure Mobile Development COD 160 Fundamentals of Secure Embedded Software Development DES 101 Fundamentals of Secure Architecture	COD 207 Communication Security in C++ COD 261 Threats to Scripts DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 255 Securing the IoT Update Process DES 260 Fundamentals of IoT Architecture and Design DES 281-290 OWASP IoT Top 10 Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations	COD 366 Creating Secure Kotlin Applications DSO 302 Automated Security Testing DSO 307 Secure Secrets Management ENG 311 Attack Surface Analysis & Reduction ENG 312 How to Perform a Security Code Review

Core Developer

The Core Developer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for the design, development, and management of applications across various environments and operating platforms and provides learners with a solid foundation of application security best practices. The Core Developer learning path covers key application security concepts including:

- Application security and risk drivers
- Essential security engineering principles: defensive coding, threat modeling, and gathering security design requirements
- How to identify and mitigate CWE's 25 most dangerous software errors

Details 42 Courses, 12 Hours, 15 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 102-108 Fundamentals of SDLC Security Series (7) COD 141 Fundamentals of Database Security DES 101 Fundamentals of Secure Architecture	DES 204 The Role of Cryptography in Application Development DES 212 Architecture Risk Analysis and Remediation DES 222-231 Applying OWASP 2017 Mitigations Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements	COD 330 Testing for Missing Authentication for Critical Function COD 332 Testing for Use of Hard-Coded Credentials COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges

	ENG 212 Implementing Secure Software Operations	COD 339 Testing for Download of Code without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String DES 311 Creating Secure Application Architecture DSO 302 Automated Security Testing DSO 307 Secure Secrets Management ENG 312 How to Perform a Security Code Review

DevOps Practitioner

The DevOps Practitioner path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those who work closely with Software Engineers to help them deploy and operate various systems. The DevOps Practitioner learning path provides teams 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.

Details 36 Courses, 13 Hours, 16 CPE Credits

Core	***Advanced***	***Elite***
COD 102-108 Fundamentals of SDLC Security Series	DES 206 Meeting Cloud Governance and Compliance Requirements	COD 383 Protecting Java Backend Services
DES 101 Fundamentals of Secure Architecture	DES 214-218 Secure Enterprise Infrastructure Series (4)	DSO 301 Orchestrating Secure System & Service Configuration
DES 151 Fundamentals of the PCI Secure SLC Standard	DSO 201 Fundamentals of Secure DevOps	DSO 302 Automated Security Testing
ENG 123 Essential Security Engineering Principles	DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework	DSO 303 Automating Security Updates
ENG 124 Essential Application Protection	DSO 253 DevSecOps in the AWS Cloud	DSO 304 Securing API Gateways in a DevSecOps Framework

ENG 125 Essential Data Protection TST 101 Fundamentals of Security Testing	DSO 254 DevSecOps in the Azure Cloud ENG 205 Fundamentals of Threat Modeling ENG 251 Risk Management Foundations TST 202 Penetration Testing Fundamentals TST 205 Performing Vulnerability Scans TST 206 ASVS Requirements for Developers	DSO 305 Automating CI/CD Pipeline Compliance DSO 306 Implementing Infrastructure as Code ENG 312 How to Perform a Security Code Review ENG 351 Preparing the Risk Management Framework

Network Engineer

The Network Engineer path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for planning, implementing and overseeing computer networks that support in-house voice, data, video and wireless network services. This learning path covers core security concepts including:

- Best practices for managing systems and services across all environments
- How to improve the stability, security, efficiency, and scalability of environments
- Gaining a baseline understanding of how to create and modify scripts to perform tasks

Details 34 Courses, 14 Hours, 16 CPE Credits

Core	***Advanced***	***Elite***
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 TST 101 Fundamentals of Security Testing	COD 261-266 Secure Scripting Series (6) DES 210 Hardening Linux/Unix Systems DES 214-218 Secure Enterprise Infrastructure Series (4) DES 260 Fundamentals of IoT Architecture and Design DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework ENG 205 Fundamentals of Threat Modeling TST 202 Penetration Testing Fundamentals TST 205 Performing Vulnerability Scans	DSO 301 Orchestrating Secure System & Service Configuration DSO 302 Automated Security Testing DS0 303 Automating Security Updates DSO 304 Securing API Gateways in a DevSecOps Framework DS0 305 Automating CI/CD Pipeline Compliance ENG 351-354 Implementing the Risk Management Framework Series (4) DSO 301 Orchestrating Secure System & Service Configuration

Automation Engineer

The Automation Engineer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those who design, program, simulate and test automated machinery and processes in order to complete exact tasks. The Automation Engineer path covers key security topics including:

- Essential goals and controls needed to create secure software
- Managing risk in the software development lifecycle
- Cryptography, handling input and output
- OWASP Top Ten

Details 42 Courses, 11 Hours, 13 CPE Credits

Core	***Advanced***	***Elite***
ENG 110 Essential Account Management Security	DES 222-231 Applying OWASP 2017 Mitigations Series (10)	COD 327 Testing for OS Command Injection
ENG 113 Essential Secure Configuration Management	DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework	COD 328 Testing for Classic Buffer Overflow
ENG 114 Essential Risk Assessment	ENG 251 Risk Management Foundations	COD 330 Testing for Missing Authentication for Critical Function
ENG 119 Essential Security Audit and Accountability		COD 332 Testing for Use of Hard-Coded Credentials
ENG 120 Essential Assessment and Authorization		COD 333 Testing for Missing Encryption of Sensitive Data
ENG 123 Essential Security Engineering Principles		COD 334 Testing for Unrestricted Upload of File with Dangerous Type
ENG 124 Essential Application Protection		COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision
ENG 125 Essential Data Protection		COD 336 Testing for Execution with Unnecessary Privileges
		COD 339 Testing for Download of Code without Integrity Check
		COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere
		COD 342 Testing for Incorrect Permission Assignment for Critical Resource
		COD 343 Testing for Use of a Potentially Dangerous Function
		COD 344 Testing for Use of a Broken or Risky Cryptographic Algorithm
		COD 345 Testing for Incorrect Calculation of Buffer Size

		COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String COD 350 Testing for Use of a One-Way Hash without a Salt DSO 302 Automated Security Testing DSO 303 Automating Security Updates DSO 306 Implementing Infrastructure as Code ENG 351 Preparing the Risk Management Framework

Embedded Test Engineer

The Embedded QA/Test Engineer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for verifying and assuring the application security of embedded systems. The Embedded QA/Test Engineer learning path provides learners with a solid understanding of applied testing techniques and a well-rounded base of knowledge to perform their tasks. This path also explores security best practices for conducting penetration tests and vulnerability assessment activities on embedded systems.

Details 52 Courses, 15 Hours, 18 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts DES 101 Fundamentals of Secure Architecture ENG 114 Essential Risk Assessment ENG 123 Essential Security Engineering Principles TST 101 Fundamentals of Security Testing	DES 212 Architecture Risk Analysis and Remediation DES 255 Securing the IoT Update Process DES 260 Fundamentals of IoT Architecture and Design ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements TST 202 Penetration Testing Fundamentals	COD 328 Testing for Classic Buffer Overflow COD 331 Testing for Missing Authorization Testing for Missing Authorization COD 332 Testing for Use of Hard-Coded Credentials COD 333 Testing for Missing Encryption of Sensitive Data COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges COD 337 Testing for Cross-Site Request Forgery

		COD 339 Testing for Download of Code Without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 345 Testing for Incorrect Calculation of Buffer Size COD 348 Testing for Uncontrolled Format String COD 349 Testing for Integer Overflow or Wraparound COD 350 Testing for Use of One-Way Hash Without A Salt COD 370-379 Testing for OWASP Top 10 Series (10) DSO 302 Automated Security Testing ENG 312 How to Perform a Security Code Review TST 301 Infrastructure Penetration Testing TST 302 Application Penetration Testing TST 351-360 Penetration Testing Series for Common Vulnerabilities and Attack Vectors (10)

QA Test Engineer

The Quality Assurance (QA)/Test Engineer learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for assessing and testing the quality of specifications and technical design.

Details 77 Courses, 23 Hours, 27 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts DES 101 Fundamentals of Secure Architecture ENG 114 Essential Risk Assessment	DES 202-205 Fundamentals of Cryptography Series (4) DES 212 Architecture Risk Analysis and Remediation DES 214-218 Secure Enterprise Infrastructure Series (4) DES 222-231 Applying OWASP 2017 Mitigations Series (10)	COD 326-350 Testing for CWE SANS Top Software Errors Series (25) COD 370-379 Testing for OWASP 2017 Series (10) DES 311 Creating Secure Application Architecture DSO 302 Automated Security Testing

ENG 123 Essential Security Engineering Principles TST 101 Fundamentals of Security Testing	ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements TST 202 Penetration Testing Fundamentals TST 205 Performing Vulnerability Scans	ENG 312 How to Perform a Security Code Review TST 351-360 Penetration Testing Series for Common Vulnerabilities and Attack Vectors (10)

IT Architect

The IT Architect learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for designing and maintaining computer networks. The IT Architect path covers key application security concepts including:

- Best practices for secure software design
- Creating integrated architecture across business and technology
- Protecting data and resources from disclosure, modification, and deletion

Details 25 Courses, 11 Hours, 13 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts DES 101 Fundamentals of Secure Architecture	DES 202 Cryptographic Suite Services: Encoding, Encrypting, and Hashing DES 206 Meeting Cloud Governance and Compliance Requirements DES 210 Hardening Linux/Unix Systems DES 212 Architecture Risk Analysis and Remediation DES 214-218 Secure Enterprise Infrastructure Series (4) DES 255 Securing the IoT Update Process DES 260 Fundamentals of IoT Architecture and Design DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework ENG 211 How to Create Application Security Design Requirements ENG 251 Risk Management Foundations	DSO 301 Orchestrating Secure System and Service Configuration DSO 304 Securing API Gateways in a DevSecOps Framework DSO 305 Automating CI/CD Pipeline Compliance DSO 306 Implementing Infrastructure as Code ENG 311 Attack Surface Analysis and Reduction ENG 351-354 Implementing the Risk Management Framework Series (4)

Embedded Architect

The Embedded Architect learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for designing and implementing software of embedded devices and systems and provides insight into the unique resource requirements of embedded environments and best practices for designing secure software for them.

Details 9 Courses, 5 Hours, 6 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security	DES 202 Cryptographic Suite Services: Encoding, Encrypting, and Hashing	DES 311 Creating Secure Application Architecture
DES 101 Fundamentals of Secure Architecture	DES 212 Architecture Risk Analysis and Remediation	ENG 311 Attack Surface Analysis & Reduction
	DES 255 Securing the IoT Update Process	ENG 312 How to Perform a Security Code Review
	DES 260 Fundamentals of IoT Architecture and Design	

Software Architect

The Software Architect learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those making design choices, coordinating and overseeing technical standards and includes software coding standards, tools, and platforms. The Software Architect path covers key application security concepts including:

- Secure software architecture best practices that can be applied to early phase SDLC activities
- Defensive coding techniques
- Avoiding systemic issues found in insecure software

Details 73 Courses, 24 Hours, 28 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security	COD 261 Threats to Scripts	COD 330 Testing for Missing Authentication for Critical Function
AWA 102 Secure Software Concepts	COD 267 Securing Python Microservices	COD 332 Testing for Hard-Coded Credentials
COD 102-108 Fundamentals of SDLC Security Series (7)	DES 202-205 Fundamentals of Cryptography Series (4)	COD 334 Testing for Unrestricted Upload of File with Dangerous Type
COD 141 Fundamentals of Database Security	DES 212 Architecture Risk Analysis and Remediation	COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision
DES 101 Fundamentals of Secure Architecture	DES 214-218 Secure Enterprise Infrastructure Series (4)	COD 336 Testing for Execution with Unnecessary Privileges
DES 151 Fundamentals of the PCI Secure SLC Standard	DES 222-231 Applying OWASP 2017 Mitigations Series (10)	COD 339 Testing for Download of Code without Integrity Check

	DES 255 Securing the IoT Update Process DES 260 Fundamentals of IoT Architecture and Design DES 281-290 OWASP IoT Top 10 Series (10) DSO 201 Fundamentals of Secure DevOps DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework ENG 211 How to Create Application Security Design Requirements ENG 251 Risk Management Foundations TST 206 ASVS Requirements for Developers	COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource COD 343 Testing for Use of a Potentially Dangerous Function COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String DES 311 Creating Secure Application Architecture DSO 301 Orchestrating Secure System & Service Configuration DSO 302 Automated Security Testing DSO 304 Securing API Gateways in a DevSecOps Framework DSO 305 Automating CI/CD Pipeline Compliance ENG 311 Attack Surface Analysis & Reduction ENG 312 How to Perform a Security Code Review ENG 351-354 Implementing the Risk Management Framework Series (4)

Business Analyst

The Business Analyst learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for defining, analyzing and documenting requirements in the software development lifecycle. The Business Analyst path covers core application security concepts including:

- Adhering to system and information security policies
- Meeting compliance mandates for relevant government and industry standards
- Access control, configuration management, risk assessment, auditing and authentication

Details 17 Courses, 6 Hours, 7 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security	DSO 201 Fundamentals of Secure DevOps	DSO 302 Automated Security Testing

AWA 102 Secure Software Concepts DES 101 Fundamentals of Secure Architecture DES 151 Fundamentals of the PCI Secure SLC Standard 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 ENG 251 Risk Management Foundations TST 202 Penetration Testing Fundamentals TST 206 ASVS Requirements for Developers	ENG 351-354 Implementing the Risk Management Framework Series (4)

Systems Analyst

The Systems Analyst learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those who specialize in the implementation of computer system requirements. The Systems Analyst learning path provides the fundamental knowledge required to secure networks and systems including:

- Taking a holistic approach to network and system security
- Defining and analyzing system problems
- Designing and testing standards and solutions
- Controls, monitoring access, operational procedures, auditing, and logging

Details 44 Courses, 13 Hours, 15 CPE Credits

Core	***Advanced***	***Elite***
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	DES 210 Hardening Linux/Unix Systems DES 222-231 Applying OWASP 2017 Mitigations Series *(10)* ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations ENG 251 Risk Management Foundations TST 206 ASVS Requirements for Developers	DSO 301 Orchestrating Secure System & Service Configuration DSO 302 Automated Security Testing DSO 304 Securing API Gateways in a DevSecOps Framework DSO 305 Automating CI/CD Pipeline Compliance ENG 351-354 Implementing the Risk Management Framework Series (4)

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		

Systems Administrator

The Systems Administrator Learning Path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for preventing and mitigating security breaches that may arise within computer systems. The Systems Administrator learning path provides a holistic approach to network and system security with an exploration of controls, monitoring access, operational procedure, and formal auditing and logging.

Details 45 Courses, 16 Hours, 20 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 141 Fundamentals of Database Security DES 151 Fundamentals of the PCI Secure SLC Standard ENG 110 Essential Account Management Security ENG 111 Essential Session Management Security ENG 113 Essential Secure Configuration Management ENG 118 Essential Incident Response ENG 119 Essential Security Audit and Accountability	COD 219 Creating Secure Code SAP ABAP Foundations COD 261-266 Secure Scripting Series (6) DES 210 Hardening Linux/Unix Systems DES 214-218 Secure Enterprise Infrastructure Series (4) DES 222-231 Applying OWASP 2017 Mitigations Series (10) DSO 201 Fundamentals of Secure DevOps DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework ENG 205 Fundamentals of Threat Modeling	DSO 301 Orchestrating Secure System & Service Configuration DSO 303 Automating Security Updates DSO 304 Securing API Gateways in a DevSecOps Framework DSO 305 Automating CI/CD Pipeline Compliance

ENG 121 Essential Identification and Authentication ENG 122 Essential Physical and Environmental Protection ENG 123 Essential Security Engineering Principles ENG 125 Essential Data Protection ENG 127 Essential Media Protection ENG 150 Meeting Confidentiality, Integrity, and Availability Requirements ENG 151 Fundamentals of Privacy Protection		

Database Administrator

The Database Administrator Learning Path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for capacity planning, installation, configuration, database design, migration, performance monitoring, security, troubleshooting, as well as back end data recovery. The Database Administrator learning path builds fundamental knowledge of secure database development including:

- Common database attacks
- Platform-specific threats
- Database secure coding best practices

Details 42 Courses, 16 Hours, 19 CPE Credits

Core	***Advanced***	COD 330 Testing for Missing Authentication for Critical Function
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts COD 141 Fundamentals of Database Security DES 101 Fundamentals of Secure Architecture	COD 241 Creating Secure Code - Oracle Database Applications COD 242 Creating Secure SQL Server and Azure SQL Database Applications COD 261 Threats to Scripts COD 262 Fundamentals of Shell and Interpreted Language Security DES 202-205 Fundamentals of Cryptography Series (4) DES 206 Meeting Cloud Governance and Compliance Requirements DES 212 Architecture Risk Analysis and Remediation	COD 332 Testing for Use of Hard-Coded Credentials COD 334 Testing for Unrestricted Upload of File with Dangerous Type COD 335 Testing for Reliance on Untrusted Inputs in a Security Decision COD 336 Testing for Execution with Unnecessary Privileges COD 339 Testing for Download of Code without Integrity Check COD 341 Testing for Inclusion of Functionality from Untrusted Control Sphere COD 342 Testing for Incorrect Permission Assignment for Critical Resource

	DES 222-231 Applying OWASP 2017 Mitigations Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements	COD 343 Testing for Use of a Potentially Dangerous Function COD 346 Testing for Improper Restriction of Excessive Authentication Attempts COD 347 Testing for Open Redirect COD 348 Testing for Uncontrolled Format String COD 352 Creating Secure jQuery Code DES 311 Creating Secure Application Architecture ENG 311 Attack Surface Analysis and Reduction ENG 312 How to Perform a Security Code Review

Linux Administrator

The Linux Administrator learning path 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.

Details 17 Courses, 7 Hours, 8 CPE Credits

Core	***Advanced***	***Elite***
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 150 Meeting Confidentiality, Integrity, and Availability Requirements	COD 261-266 Secure Scripting Series (6) DES 214 Securing Infrastructure Architecture DES 215 Defending Infrastructure DES 260 Fundamentals of IoT Architecture and Design ENG 205 Fundamentals of Threat Modeling	

Product Owner

The Product Owner learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for setting,

prioritizing, and evaluating the work generated by a software Scrum team to ensure impeccable features and functionality of the product. The Product Owner learning path introduces application security fundamentals including the essentials goals and controls needed to create secure software and manage risk in the software development lifecycle.

Details 33 Courses, 11 Hours, 13 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security	DES 222-231 Applying OWASP 2017 Mitigations Series (10)	DSO 302 Automated Security Testing
AWA 102 Secure Software Concepts	DES 212 Architecture Risk Analysis and Remediation	ENG 311 Attack Surface Analysis and Reduction
DES 151 Fundamentals of the PCI Secure SLC Standard	DES 260 Fundamentals of IoT Architecture and Design	ENG 351 Preparing the Risk Management Framework
ENG 124 Essential Application Protection	DSO 201 Fundamentals of Secure DevOps	
ENG 125 Essential Data Protection	ENG 211 How to Create Application Security Design Requirements	
ENG 150 Meeting Confidentiality, Integrity, and Availability Requirements	ENG 251 Risk Management Foundations	
ENG 151 Fundamentals of Privacy Protection	TST 202 Penetration Testing Fundamentals	
ENG 191-195 Implementing the MS SDL into your SDLC Series (5)	TST 206 ASVS Requirements for Developers	
TST 101 Fundamentals of Security Testing		

Project Manager

The Project Manager learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It introduces project managers to the essentials of access control, configuration management, risk assessment, auditing, and authentication. It also provides the knowledge and skills necessary to ensure adherence to your organization's system and information security policies as well as relevant governmental and industry standards.

Details 36 Courses, 13 Hours, 16 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security	DES 204 The Role of Cryptography in Application Development	DSO 301 Orchestrating Secure System & Service Configuration
AWA 102 Secure Software Concepts	DES 206 Meeting Cloud Governance and Compliance Requirements	DSO 302 Automated Security Testing
COD 102-108 Fundamentals of SDLC Security Series (7)	DES 212 Architecture Risk Analysis and Remediation	DSO 305 Automating CI/CD Pipeline Compliance
COD 141 Fundamentals of Database Security*	DES 214-218 Secure Enterprise Infrastructure Series (4)	ENG 312 How to Perform a Security Code Review
COD 152 Fundamentals of Secure Cloud Development*	DSO 201 Fundamentals of Secure DevOps	ENG 351 Preparing the Risk Management Framework

DES 101 Fundamentals of Secure Architecture DES 151 Fundamentals of the PCI Secure SLC Standard ENG 123 Essential Security Engineering Principles ENG 124 Essential Applications Protection ENG 125 Essential Data Protection ENG 150 Meeting Confidentiality, Integrity, and Availability Requirements ENG 151 Fundamentals of Privacy Protection	DSO 206 Securing the Open-Source Software Supply Chain DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 251 Risk Management Foundations TST 206 ASVS Requirements for Developers	

Cyber Security Professional

The Cybersecurity Professional learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those tasked with everything from the technical aspects of security, security policy and everything in between.

Details 10 Courses, 3 Hours, 4 CPE Credits

Core	***Advanced***	***Elite***
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 ENG 151 Fundamentals of Privacy Protection TST 101 Fundamentals of Software Security Testing	DES 206 Meeting Cloud Governance and Compliance Requirements TST 202 Penetration Testing Fundamentals TST 206 ASVS Requirements for Developers	

Operations/IT Manager

The Operations/IT Learning Path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for managing operations and sharing responsibility for project success and managing day-to-day IT processes. The Operations/IT Manager path covers key security concepts including:

- Essential goals and controls needed for secure software development
- Managing risk associated with the software development lifecycle
- Developing, implementing, and ensuring compliance with operational application security policies and procedures

Details 39 Courses, 14 Hours, 16 CPE Credits

Core	***Advanced***	***Elite***
DES 151 Fundamentals of the PCI Secure SLC Standard	DES 206 Meeting Cloud Governance and Compliance Requirements	DSO 301 Orchestrating Secure System & Service Configuration
ENG 110 Essential Account Management Security	DES 210 Hardening Linux/Unix Systems	DSO 302 Automated Security Testing
ENG 111 Essential Session Management Security	DES 214-218 Secure Enterprise Infrastructure Series (4)	DSO 303 Automating Security Updates
ENG 112 Essential Access Control for Mobile Devices	DSO 201 Fundamentals of Secure DevOps	DS0 305 Automating CI/CD Pipeline Compliance
ENG 113 Essential Secure Configuration Management	DSO 205 Securing the COTS Supply Chain	
ENG 114 Essential Risk Assessment	DSO 206 Securing the Open-Source Software Supply Chain	
ENG 115 Essential System and Information Integrity	DSO 211 Identifying Threats to Containers and Data in a DevSecOps Framework	
ENG 116 Essential Security Planning Policy and Procedures	ENG 205 Fundamentals of Threat Modeling	
ENG 117 Essential Information Security Program Planning	TST 202 Penetration Testing Fundamentals	
ENG 118 Essential Incident Response	TST 205 Performing Vulnerability Scans	
ENG 119 Essential Security Audit and Accountability	TST 206 ASVS Requirements for Developers	
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 150 Meeting Confidentiality, Integrity, and Availability Requirements		
ENG 151 Fundamentals of Privacy Protection		

Application Security Champion

The Application Security Champion learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those chartered with driving a culture of "Security Built-in" to the software development lifecycle. The Application Security Champion learning path also explains application security concepts such as privacy, secure development and architecture, security testing, threat modeling, cryptography, and cyber threat analysis and remediation.

Details 33 Courses, 10 Hours, 12 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security	DES 204 The Role of Cryptography in Application Development	DSO 302 Automated Security Testing
AWA 102 Secure Software Concepts	DES 212 Architecture Risk Analysis and Remediation	ENG 311 Attack Surface Analysis and Reduction
COD 102-108 Fundamentals of SDLC Security Series (7)	DES 222-231 Applying OWASP 2017 Mitigations Series (10)	ENG 312 How to Perform a Security Code Review
ENG 124 Essential Application Protection	ENG 205 Fundamentals of Threat Modeling	
ENG 125 Essential Data Protection	ENG 211 How to Create Application Security Design Requirements	
ENG 150 Meeting Confidentiality, Integrity, and Availability Requirements	TST 202 Penetration Testing Fundamentals	
ENG 151 Fundamentals of Privacy Protection	TST 206 ASVS Requirements for Developers	
TST 101 Fundamentals of Security Testing		

Information Security Specialist

The Information Security Specialist learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for protecting systems, defining access privileges, control structures, and resources. The Information Security Specialist learning path helps build the skills required to identify, protect, detect and recover from risks, vulnerabilities, and threats to the security of information and/or data.

Details 50 Courses, 16 Hours, 19 CPE Credits

Core	***Advanced***	***Elite***
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts	COD 241 Creating Secure Code Oracle Foundations COD 242 Creating Secure SQL Server & Azure SQL Database Applications	ENG 311 Attack Surface Analysis and Reduction ENG 312 How to Perform a Security Code Review

COD 141 Fundamentals of Database Security DES 151 Fundamentals of the PCI Secure SLC Standard 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 151 Fundamentals of Privacy Protection TST 101 Fundamentals of Security Testing	COD 246-249 PCI Compliance for Developers Series (4) COD 256 Creating Secure Code Ruby on Rails Foundations COD 261 Threats to Scripts DES 206 Meeting Cloud Governance and Compliance Requirements DES 212 Architecture Risk Analysis and Remediation DES 271-280 OWASP Mobile Top Ten Series (10) ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements ENG 212 Implementing Secure Software Operations TST 206 ASVS Requirements for Developers	

Systems Leadership

The Systems Leadership learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for computers and their complex operating systems. It also builds the baseline but comprehensive application security knowledge necessary for leading application development and design projects. The Systems Leadership learning path explores application security best practices necessary to ensure strategies and plans support business needs and align with departmental and organizational objectives

and goals.

Details 21 Courses, 7 Hours, 8 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts DES 151 Fundamentals of the PCI Secure SLC Standard	DES 206 Meeting Cloud Governance and Compliance Requirements DES 222-231 Applying OWASP 2017 Mitigations Series (10) DSO 201 Fundamentals of Secure DevOps TST 206 ASVS Requirements for Developers	DES 311 Creating Secure Application Architecture DSO 301 Orchestrating Secure System & Service Configuration DSO 302 Automated Security Testing DSO 303 Automating Security Updates DSO 305 Automating CI/CD Pipeline Compliance

Development Manager

The Development Manager's learning path includes a variety of security courses that will vary depending on whether you are seeking core, advanced or elite paths. It is designed for those responsible for planning, preparing and ensuring that projects are completed. The Development Manager's learning path introduces application security best practices required to adhere to system and information security policies and compliance. Learners can apply these best practices to the requirements, design, and implementation phases of the software development lifecycle.

Details 21 Courses, 8 Hours, 9 CPE Credits

Core	*Advanced*	*Elite*
AWA 101 Fundamentals of Application Security AWA 102 Secure Software Concepts DES 101 Fundamentals of Secure Architecture DES 151 Fundamentals of the PCI Secure SLC Standard ENG 110 Essential Account Management Security ENG 114 Essential Risk Assessment ENG 117 Essential Information Security Program Planning ENG 151 Fundamentals of Privacy Protection ENG 191-195 Implementing the MS SDLC into your SDLC Series (5)	DES 255 Securing the IoT Update Process DES 260 Fundamentals of IoT Architecture and Design DSO 201 Fundamentals of Secure DevOps ENG 205 Fundamentals of Threat Modeling ENG 211 How to Create Application Security Design Requirements TST 206 ASVS Requirements for Developers	DSO 302 Automated Security Testing DSO 305 Automating CI/CD Pipeline Compliance