Certified Application Security Engineer Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Certified Application Security Engineer Training Course is engineered to transform developers and security professionals into Secure Software Development Lifecycle experts. Participants will master proactive security strategies, moving beyond reactive patching to fully integrate DevSecOps practices and Threat Modeling from the initial design phase. We deliver hands-on, expert-led instruction focusing on mitigating the OWASP Top 10 and leveraging Static and Dynamic analysis tools to build Resilient, Cloud-Native applications. The CASE certification validates a professional's ability to ensure application-level security, a critical skill in today's Zero Trust architecture environments.

The modern digital landscape demands that security is a core, non-negotiable element of software development. Our course equips engineers with the Defensive Coding Practices and architectural principles necessary to prevent costly security breaches and ensure regulatory Compliance. You'll gain practical experience in Vulnerability Assessment, Remediation, and automated security integration into CI/CD Pipelines. By focusing on real-world Case Studies and current attack vectors, we prepare you to immediately contribute to a stronger Application Security Posture within any enterprise, making you an indispensable asset in the fight against sophisticated cyber threats.

Programme Curriculum

Certified Application Security Engineer Training Course

Introduction

Certified Application Security Engineer Training Course is engineered to transform developers and security professionals into Secure Software Development Lifecycle experts. Participants will master proactive security strategies, moving beyond reactive patching to fully integrate DevSecOps practices and Threat Modeling from the initial design phase. We deliver hands-on, expert-led instruction focusing on mitigating the OWASP Top 10

and leveraging Static and Dynamic analysis tools to build Resilient, Cloud-Native applications. The CASE certification validates a professional's ability to ensure application-level security, a critical skill in today's Zero Trust architecture environments.

The modern digital landscape demands that security is a core, non-negotiable element of software development. Our course equips engineers with the Defensive Coding Practices and architectural principles necessary to prevent costly security breaches and ensure regulatory Compliance. You'll gain practical experience in Vulnerability Assessment, Remediation, and automated security integration into CI/CD Pipelines. By focusing on real-world Case Studies and current attack vectors, we prepare you to immediately contribute to a stronger Application Security Posture within any enterprise, making you an indispensable asset in the fight against sophisticated cyber threats.

Course Duration

5 days

Course Objectives

1. Master the Secure Software Development Lifecycle and its integration within Agile and DevSecOps frameworks.
2. Perform advanced Threat Modeling and Risk Assessment for complex, multi-tiered applications.
3. Implement Secure Coding Practices to mitigate the entire OWASP Top 10 and emerging threats.
4. Design and architect Cloud-Native and Microservices applications with security-by-design principles.
5. Conduct effective Static Application Security Testing and Dynamic Application Security Testing (DAST).
6. Securely implement and manage Authentication, Authorization, and Identity and Access Management systems.
7. Integrate automated security checks, including Security as Code, into CI/CD Pipelines.
8. Apply Cryptography and Key Management best practices to protect data-at-rest and data-in-transit.
9. Develop robust Logging, Monitoring, and Secure Error Handling mechanisms for prompt incident detection.
10. Understand and ensure application adherence to global Data Protection and regulatory Compliance standards.
11. Perform Vulnerability Assessment and prioritize Remediation efforts based on business risk.
12. Secure API Endpoints and understand the risks associated with modern web frameworks.
13. Establish a proactive Application Security Program and foster a Security Champion culture.

Target Audience

1. Software Developers/Engineers.
2. Application Security Specialists/Analysts.
3. Security Engineers.
4. DevOps and DevSecOps Engineers.
5. Quality Assurance Engineers and Penetration Testers.
6. Software Architects.
7. Technical Project Managers/IT Managers.
8. Cybersecurity Consultants.

Course Modules

Module 1: Foundations of Secure SDLC & Threat Modeling

- Integrating Security Gates into the Agile and DevSecOps workflows.
- Introduction to the Secure Software Development Lifecycle models.
- Principles of Security-by-Design and Shift-Left security.
- Methodologies for Threat Modeling and risk ranking.
- Case Study: Equifax Data Breach (2017).

Module 2: Secure Application Design and Architecture

- Architectural considerations for Microservices and Serverless environments.
- Implementing the Zero Trust model for application access and segmentation.
- Best practices for API Security.
- Secure configuration of application components and third-party dependencies.
- Case Study: Capital One Breach (2019).

Module 3: Secure Coding Practices: Injection & Data Validation

- In-depth defense against all Injection flaws.
- Implementing comprehensive Input Validation, Output Encoding, and data sanitization.
- Secure handling of file uploads and deserialization attacks.
- Mitigation of Cross-Site Scripting and Cross-Site Request Forgery.
- Case Study: Heartland Payment Systems Breach (2008).

Module 4: Authentication, Authorization, and Session Management

- Implementing Multi-Factor Authentication and strong password policies.
- Best practices for Identity and Access Management and OAuth 2.0/OIDC flows.
- Secure Session Management including token handling, expiration, and revocation.
- Preventing Broken Access Control vulnerabilities.
- Case Study: T-Mobile Data Breach (2021).

Module 5: Cryptography and Sensitive Data Protection

- Choosing and implementing appropriate Cryptographic Algorithms
- Secure Key Management practices and storage
- Data protection regulations and Compliance
- Securing data-at-rest and data-in-transit
- Case Study: Target Data Breach (2013).

Module 6: Security Testing (SAST, DAST, IAST)

- Integrating Static Application Security Testing tools into development workflows.
- Performing Dynamic Application Security Testing and fuzzing.
- Introduction to Interactive Application Security Testing and SCA
- Automating Vulnerability Scanning and integrating results into issue trackers.
- Case Study: Log4Shell Vulnerability (2021).

Module 7: Security Automation and DevSecOps Integration

- Writing Security as Code using policies and frameworks
- Automating security controls within CI/CD Pipelines
- Implementing continuous Security Monitoring and alerting.
- Container and Orchestration Security

- Case Study: Codecov Compromise (2021).

Module 8: Post-Deployment Security, Logging, and Incident Response

- Best practices for Secure Configuration and patch management in production.
- Implementing Security Logging and Auditing using technologies like SIEM.
- Designing and testing a tailored Application Security Incident Response Plan.
- Techniques for secure Error Handling to prevent information leakage.
- Case Study: SolarWinds Attack (2020).

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com