Training: Mile2
C)SWAE - Certified Secure Web Application Engineer

TRAINING GOALS:

The Mile2 Certified Secure Web Application Engineer (CSWAE), course prepares developers, software engineers, DevSecOps professionals, application security teams, and technical managers to build and maintain secure web applications. Students learn secure design, threat modeling, authentication, authorization, session security, secure data handling, logging, deployment security, CI/CD protection, software supply chain security, and risk-based application defense across the full lifecycle.

CSWAE also connects modern web application security practices to the OWASP Top 10, instructing students to understand how risks such as broken access control, injection, misconfiguration, cryptographic failures, authentication weaknesses, and supply chain issues occur and how to prevent them. Through live hands-on practical labs using tools such as OWASP ZAP, students validate controls, identify weaknesses, strengthen secure development practices, and improve real-world application security readiness.

Upon completion

- Upon completion, the Certified Secure Web Application Engineer candidate will understand how to support secure web application design, development, testing, deployment, and monitoring. Students will apply secure coding principles, reduce application risks, and align controls with OWASP guidance and DevSecOps practices.

Each participant in an authorized Mile2 C)SWAE training held in Compendium CE will receive a free CSWAE Certified Secure Web Application Engineer exam voucher.

Who Should Attend

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Mile2® is:

- ACCREDITED by the NSA CNSS 4011-4016 https://mile2.com/accreditations/
- MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework https://mile2.com/niccs/
- APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

CONSPECT:

- Module 01: Security Mindset, Risk, and Threat Modeling
  - The Security Mindset
  - Core Security Principles
  - Risk Thinking and Secure Design Assumptions
  - Threat Modeling with STRIDE
  - Collaborative Application Risk Analysis
  - Building a Culture of Prevention
- Module 02: Secure Foundations: Architecture, Transport, and Headers
  - Secure Architecture and Trust Boundaries
  - Segmentation and Zero Trust Thinking
  - HTTPS and TLS Basics
  - Certificate Trust and Common TLS Risks
  - HTTP Security Headers
  - Centralized Header Management
  - Leadership and Secure Defaults
- Module 03: Authentication and Session Security
  - Authentication Principles
  - Common Authentication Weaknesses
  - Password Hygiene and Secure Storage
  - Multi-Factor Authentication
  - OAuth 2.0 and OpenID Connect
  - Session Management

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Cookie Security
- JWTs and Token-Based Sessions
- Leadership Practices for Identity Security

- Module 04: Authorization and Access Control
  - Principles of Authorization
  - Least Privilege and Separation of Duties
  - Role-Based Access Control
  - Attribute-Based Access Control
  - Policy-Based Access Control
  - Broken Access Control
  - Insecure Direct Object References
  - Privilege Escalation
  - Sustaining Secure Access Practices
- Module 05: Secure Input and Data Validation
  - Foundations of Secure Input
  - Untrusted Input Sources
  - Validation, Sanitization, and Encoding
  - Cross-Site Scripting
  - Injection Attacks
  - Unsafe File Uploads
  - Deserialization and Structured Data Risks
  - Allowlists, Normalization, and Schema Validation
  - Output Encoding by Context
  - Testing Input Defenses with OWASP ZAP
- Module 06: Secure Data Handling and Storage
  - Understanding Sensitive Data
  - Data Classification Levels
  - Hashing vs. Encryption
  - Modern Password Hashing
  - Encryption at Rest
  - Secrets, Keys, and Environment Configuration
  - Common Data Storage Failures
  - Logging and Caching Sensitive Data
  - Data Minimization and Secure Retention
  - Role-Based Responsibility for Data Safety
- Module 07: Monitoring, Detection, and Logging

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Why Monitoring Matters
- Logs, Metrics, and Traces
- Good Logging Principles
- Structured vs. Unstructured Logging
- Correlation IDs
- Metrics and System Health
- Traces in Distributed Systems
- Signal vs. Noise
- Common Logging Failures
- Detection, Alerting, and Operational Visibility

- Module 08: Secure Deployment and Configuration Management
  - Why Deployment Security Matters
  - Secure Configuration Principles
  - Environment Separation
  - Least Privilege for Services and Containers
  - Secrets Management
  - Configuration Files and Environment Variables
  - Patching, Dependencies, and Version Control
  - Common Misconfigurations
  - Debug Mode, Default Credentials, and Exposed Services
  - Configuration Validation and Deployment Governance
- Module 09: Secure CI/CD and Supply Chain Security
  - Why CI/CD Security Matters
  - The CI/CD Attack Surface
  - Least Privilege for Pipelines
  - Dependency Trust and Verification
  - Artifact Integrity and Build Authenticity
  - SBOM and Supply Chain Visibility
  - Secrets in CI/CD
  - Privileged or Persistent Build Runners
  - Pipeline Hardening and Governance
  - Secure Promotion from Source to Deployment
- Module 10: Incident Response and Recovery for Web Applications
  - Why Incident Response Matters
  - Recognizing a Security Incident
  - Detection vs. Confirmation

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Incident Response Lifecycle
- Containment Without Destroying Evidence
- Eradication and Recovery
- Lessons Learned and Blameless Review
- Common Response Failures
- Communication and Role Clarity
- Building Response Readiness into Web Teams

- Module 11: OWASP Top 10: Mapping Risk to Practice
  - Why OWASP Top 10 Exists
  - How OWASP Is Commonly Misused
  - How This Course Approaches OWASP
  - Broken Access Control
  - Security Misconfiguration
  - Software Supply Chain Failures
  - Cryptographic Failures
  - Injection
  - Insecure Design
  - Authentication Failures
  - Software or Data Integrity Failures
  - Logging and Monitoring Failures
  - SSRF and Emerging Web Risks
  - OWASP Mapping, Audit Translation, and Capstone Reflection
- Lab 00: Lab Introduction
  - Recording IPs and Logging In
- Lab 01: Threat Modeling & Secure Foundations
  - Observing the Unauthenticated Application
  - Exploring the Application as an Authenticated User
  - Modeling Threats Without Exploitation
  - Observing and Testing Trust Assumptions with OWASP ZAP
  - Categorizing and Prioritizing Risk
- Lab 02: Securing Transport and Headers in a Web Application
  - Get the Application
  - Run the Application Behind Nginx
  - Generate a Local Certificate
  - Configure Nginx for HTTPS and Headers
  - Start the Environment

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Verify Headers and TLS with OWASP ZAP
- Reflect and Record

- Lab 03: Authentication and Session Security
  - Baseline Authentication and Session Observation
  - Session Cookie Analysis
  - Score Board Discovery
  - Authentication Injection
  - Broken Account Recovery
  - Password Policy Evaluation
  - Session Fixation and Rotation Testing
- Lab 04: Authorization & Access Control
  - Authorization Surface Mapping
  - Baseline Authorization Behavior
  - Horizontal Authorization
  - Vertical Authorization
  - Horizontal vs Vertical Classification
  - Authorization Rule Definition
  - Authorization Test Matrix
  - Defense-in-Depth Review
- Lab 05: Operation Clean Input: Securing the Data Pipeline
  - Intelligence Gathering: Input Surface Mapping
  - The Pop-Up Incident: XSS Exploration
  - The Skeleton Key: Injection Testing
  - The Trojan Horse: File Upload Validation
  - The Shield Wall: Mitigation Mapping
  - The Blueprint: Defense-in-Depth Design
  - The Final Inspection: Verification with ZAP
- Lab 06: Operation Silent Vault: Securing Data at Rest and in Transit
  - Intelligence Gathering: Data Surface Mapping
  - The Log Leak: Plaintext Exposure Discovery
  - The Credential Vault: Password Hashing Analysis
  - The Forgotten Key: Secrets & Configuration Review
  - The Trojan Upload: File Upload Data Handling
  - The Shield Blueprint: Mitigation Mapping via Coding Challenges
  - The Vault Protocol: Defense-in-Depth Design
  - The Final Audit: Verification with ZAP

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Lab 07: Operation Glass House: Illuminating the Dark Corners
  - Intelligence Gathering: Log Surface Mapping
  - The Secret Leak: Sensitive Data Discovery
  - The Noise Wall: Signal vs. Noise Analysis
  - The Broken Trail: Correlation & Context
  - The Shield Blueprint: Mitigation Mapping
  - The Visibility Protocol: Logging Policy Design
  - The Final Audit: Verification Simulation
- Lab 08: Operation Hardened Shell: Securing Deployment & Configuration
  - Intelligence Gathering: Container Surface Mapping
  - The Debug Door: Verbose Error Exposure
  - The Secret Leak: Hardcoded Credentials Hunt
  - The Root Risk: Least Privilege Testing
  - The Shield Blueprint: Mitigation Mapping
  - The Fortification: Hardening the Deployment
  - The Final Audit: Verification with ZAP
- Lab 09: Operation Trusted Factory: Securing the Supply Chain
  - Artifact Inspection: Layer & History Analysis
  - The Secret Leak: CI Log & Config Exposure
  - Dependency Trust: Vulnerable Libraries
  - Artifact Integrity: Hashing & Verification
  - The Shield Blueprint: Mitigation Mapping
  - The Pipeline Protocol: CI/CD Security Policy Design
  - The Final Audit: Verification Simulation
- Lab 10: Operation Calm Center: Incident Response & Recovery
  - Detection & Analysis: Signal vs. Noise
  - Declaration & Communication
  - Containment: Stop the Bleeding
  - Evidence Preservation
  - Recovery & Verification
  - Lessons Learned

REQUIREMENTS:

Suggested prerequisites:

- Sound knowledge of networking

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- At least one coding language
- Linux understanding
- Open shell

or 24 months experience in software technologies and security.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Mile2 (course completion).

This course will help prepare you for the Certified Secure Web Application Engineer CSWAE exam, which is available through the on-line Mile2's Learning Management System, and is accessible on your mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions. A minimum grade of 70% is required for certification.

Each participant in an authorized Mile2 C)SWAE training held in Compendium CE will receive a free CSWAE Certified Secure Web Application Engineer exam voucher.

TRAINER:

Certified Mile2 Instructor

ADDITIONAL INFORMATION:

Course Student Kit includes:

- Digital Workbook & Study Guide – training materials in the digital form (1-year access)
- Live Cyber Range Labs – cloud-based lab environment (2-week access)
- Exam Prep Guide + Practice Questions – additional materials to help you prepare for the exam
- Official Certification Exam (2 Attempts Included) – exam voucher, with a second free attempt if needed

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007