OWASP CYCLONEDX TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP CycloneDX & SBOM

- What is CycloneDX and its role in software supply chain security
- SBOM fundamentals and terminology
- Why SBOMs are critical (Log4Shell, SolarWinds, etc.)
- CycloneDX vs SPDX - key differences

CycloneDX Specification & Core Concepts

- CycloneDX specification overview
- Supported formats: JSON, XML, Protobuf
- Component types (libraries, containers, services, files)
- Metadata, components, dependencies, and services

Components, Dependencies & Dependency Graphs

- Identifying direct vs transitive dependencies
- Dependency trees and graphs
- Handling multiple languages and ecosystems
- Managing third-party and open-source components

Generating SBOMs with CycloneDX Tools

- CycloneDX CLI overview
- Language-specific tools (Maven, Gradle, npm, Python, Go, .NET)
- Container and image SBOM generation
- Hands-on: Generate an SBOM for a sample application

SBOM Quality, Accuracy & Best Practices

- Common SBOM generation mistakes
- Ensuring completeness and correctness
- Versioning and lifecycle management
- SBOM storage and distribution

DAY 2

Vulnerability & Risk Management with CycloneDX

- Integrating SBOMs with vulnerability databases
- CVE, CWE, and exploitability context
- Tracking vulnerable components
- Continuous risk monitoring

CycloneDX VEX (Vulnerability Exploitability eXchange)

- Introduction to VEX
- Vulnerability status: affected, not affected, fixed
- Using VEX with CycloneDX
- Reducing false positives

License Compliance & Legal Risk Management

- License metadata in CycloneDX
- Open-source license risks
- License policy enforcement
- Legal and compliance use cases

CycloneDX in CI/CD & DevSecOps Pipelines

- SBOM generation in CI/CD pipelines
- Integrating with SCA tools
- Policy gates and security automation
- Secure SDLC integration

Container, Cloud-Native & Microservices SBOMs

- Container image SBOMs
- Kubernetes and cloud-native environments
- Service and API SBOMs
- Managing SBOMs at scale

Compliance, Regulations & Industry Standards

- SBOM requirements (NIST, NTIA, EO 14028)
- Mapping CycloneDX to ISO, SOC 2, PCI DSS
- Supplier and third-party risk management
- SBOM exchange with vendors

Real-World Use Cases & Implementation Strategy

- Enterprise SBOM adoption roadmap
- Case studies and lessons learned
- Common challenges and solutions
- Tooling ecosystem overview