



WORKSHOP

DevSecOps und sichere Software-Lieferketten

3 Tage · 16 Module

www.HCO.de · Gesamtfoliensatz

HECKER
CONSULTING



KAPITEL 1

Die Module

Die Software-Lieferkette vom Commit bis zum Deployment absichern





Module 1 bis 9

Nr.	Modul
1	Die moderne Software-Lieferkette
2	Bedrohungsmodell für die Lieferkette
3	DevSecOps, Secure by Design und NIST SSDF
4	Repository und Entwicklungsprozess absichern
5	Abhängigkeiten und Paketquellen kontrollieren
6	Security Scanning in der Pipeline
7	Pipelines härten und Berechtigungen reduzieren
8	Reproduzierbare und nachvollziehbare Builds
9	Grundlagen der Software Bill of Materials



Module 10 bis 16

Nr.	Modul
10	SPDX und CycloneDX praktisch einsetzen
11	Schwachstellenmanagement mit SBOM und VEX
12	Signaturen, Attestierungen und Provenance
13	SLSA 1.2 in der Praxis
14	Container, Registry und Deployment absichern
15	Schwachstellenmeldungen und Security Incident Response
16	Cyber Resilience Act und dauerhaftes Betriebsmodell



Für wen dieses Seminar ist

- › Softwareentwicklerinnen und -entwickler, Software- und Lösungsarchitekten, DevOps-, Platform- und Cloud-Engineers, Build- und Release-Verantwortliche, Application- und Product-Security-Spezialisten sowie technische Projektleitungen, die Sicherheit in Entwicklung, Build und Auslieferung verankern wollen.



Was Ihr Team danach kann

- › Angriffsflächen und Vertrauensgrenzen einer Software-Lieferkette identifizieren und ein projektspezifisches Bedrohungsmodell erstellen
- › NIST SSDF und OWASP SAMM auf ein konkretes Projekt übertragen und Repository, Branches und Releases angemessen schützen
- › Risiken direkter und transitiver Abhängigkeiten bewerten sowie Dependency Confusion und Typosquatting erschweren



Was Ihr Team danach kann (Fortsetzung)

- › SAST, SCA, Secret-, IaC- und Container-Scanning sinnvoll kombinieren und mit tragfähigen Quality Gates steuern
- › CI/CD-Berechtigungen, Runner, Secrets und Caches härten und Builds reproduzierbar und nachvollziehbar machen
- › SBOMs in SPDX und CycloneDX erzeugen, auf Qualität prüfen und Schwachstellen mit VEX nach Risiko priorisieren



Was Ihr Team danach kann (Fortsetzung)

- › Build-Provenance und Attestierungen erstellen, Artefakte mit Cosign signieren und vor dem Deployment verifizieren
- › SLISA-Reifegrade beurteilen, eine Gap-Analyse erstellen und technische Nachweise für Audit-, Kunden- und CRA-Prozesse vorbereiten



Was Ihr Team mitbringen sollte

- › Grundlegende Erfahrung mit Git und Pull Requests
- › Den prinzipiellen Ablauf einer CI/CD-Pipeline kennen
- › Anwendungen mit einem Paket- oder Build-Manager erstellen können



Was Ihr Team mitbringen sollte (Fortsetzung)

- › Grundkenntnisse zu Containern und Docker
- › Grundsätzliche Vertrautheit mit typischen Software-Schwachstellen
- › Kein Vorwissen zu SLSA, SBOM, Sigstore oder dem Cyber Resilience Act nötig



Sprechen Sie uns an

- › HECKER CONSULTING · Erkrather Str. 401 · 40231 Düsseldorf
- › Telefon: +49 211 542 480 40
- › E-Mail: info@hco.de
- › www.learning-master.de

