LI560 Kubernetes Security

Kurzbeschreibung:

In diesem Kurs lernen die Teilnehmer Kubernetes-Cluster und containerisierte Workloads ganzheitlich abzusichern – von Architektur über Netzwerk- und Laufzeitsicherheit bis zu Supply-Chain und Compliance. Hands-On-Labs und Best Practices vermitteln praxisnah, wie resilienter und sicherer Betrieb von Kubernetes gelingt.

Zielgruppe:

- DevOps-/Platform Engineers
- Administratoren
- Security- und Compliance-Spezialisten
- Entwickler
- Penetration Tester
- Red Teams

Voraussetzungen:

Um Kursinhalten und Lerntempo des Workshops **LI560 Kubernetes Security** gut folgen zu können, sind zwingend gute Linux- und Kubernetes-Kenntnisse nötig.

Wir empfehlen Ihnen den vorherigen Besuch der folgenden Kurse:

- LI500 Container Grundlagen
- LI510 Kubernetes Basics
- LI530 Kubernetes Advanced

Sonstiges:

Dauer: 5 Tage

Preis: 3650 Euro plus Mwst.

Ziele:

- Sicherheitsverständnis aufbauen: Sie lernen, Bedrohungsmodelle und Angriffsvektoren zu analysieren und die sicherheitsrelevante Architektur von Kubernetes einzuordnen.
- Best Practices anwenden: Sie lernen, wie Control Plane, Workloads und Netzwerke gehärtet werden können – von RBAC über Pod Security bis zu Container- und Runtime-Schutzmaßnahmen.
- Compliance sicherstellen: Der Kurs vermittelt Methoden, um regulatorische Anforderungen (z. B. CIS Benchmarks, Audit Logging, SBOM, Signaturen) in Kubernetes-Umgebungen umzusetzen.
- Praxis durch Hands-On-Labs: Sie üben reale Angriffsszenarien, Abwehrmaßnahmen und Incident Response, um Sicherheit in der Praxis anzuwenden.
- Ganzheitliche Sicht entwickeln: Sie gewinnen die Fähigkeit, Kubernetes-Sicherheit entlang der gesamten Supply Chain zu betrachten – vom Code bis zum Betrieb im Cluster.

Inhalte/Agenda:

- ♦ **Cluster Security**
  - ♦ ◊ Kubernetes Archiktur
  - ◊ Bedrohungsmodell & Angriffsvektoren
  - ◊ ControlPlane Hardening & Admission Controller
  - ◊ RBAC & ServiceAccounts
  - ◊ Pod Security Admission
  - ◊ CIS Benchmark
  - ◊ Workload Node Security

- ♦ **Netzwerk & Container Security (Cluster & Container Ebene)**
  - ♦ ◊ CNI & Netzwerkübersicht
  - ◊ Container-Härtung & Image Security
  - ◊ Policy Engines
  - ◊ ServiceMesh

- ♦ **Runtime & Monitoring (Container & Cluster Ebene)**
  - ♦ ◊ Shift-left-Security
  - ◊ Runtime Security Basics (seccomp, AppArmor, Capabilities)
  - ◊ Falco: Syscall-basiertes Monitoring (Syscall Monitoring)
  - ◊ Kubernetes Audit Logging
  - ◊ Incident Response & Forensik (Hands-On Lab)

- ♦ **Supply◊Chain & Compliance (Code Ebene & Integration)**
  - ♦ ◊ Container Scanning & Software Bill of Materials (SBOM)
  - ◊ Image Signaturen & Verifikation
  - ◊ Compliance & Automatisierung
  - ♦ ◊