

Trainings

Kubernetes Security Fundamentals



Security

Dieses Training betrachtet die Security-Aspekte des gesamten Cluster Lifecycles: von initialer Konfiguration und Deployment, über Betrieb, bis hin zum Umgang mit neu entdeckten bzw. veröffentlichten Schwachstellen.

Dauer: 4 Tage

Zielgruppe: Kubernetes-Administrator:innen mit guten Linux-Kenntnissen

Kubernetes hat sich in den letzten Jahren als Standard-Framework für die zugrunde liegende Infrastruktur von SaaS (Software as a Service) -Produkten etabliert. Nahezu alle Unternehmen stellen ihren Entwicklern Kubernetes Cluster als Betriebsumgebung, in einer eigenen oder einer Public Cloud, zur Verfügung. Eine notwendige Voraussetzung für den sicheren Betrieb solcher SaaS-Produkte ist ein sicherer Kubernetes Cluster. Ein Kubernetes Cluster ist aber ein komplexes System, bei dem es nicht ausreicht, immer nur die neuesten Security-Patches einzuspielen.

Dieses Training betrachtet die Security-Aspekte des gesamten Cluster Lifecycles: von initialer Konfiguration und Deployment, über Betrieb, bis hin zum Umgang mit neu entdeckten bzw. veröffentlichten Schwachstellen (CVEs). Zudem wird thematisiert, wie Deployment Pipelines für SaaS-Produkte designt werden können, um typische Supply-Chain-Angriffe zu verhindern.

Wie alle Trainings der inovex Academy wird auch in diesem Training ein Fokus auf Praktisches Lernen gelegt: Die Teilnehmer:innen designen und bauen im Laufe des Trainings einen eigenen, sicheren Kubernetes Cluster auf und implementieren dort Security Monitoring und Logging.

Zielgruppe:

Kubernetes-Administrator:innen mit guten Linux-Kenntnissen. Voraussetzung ist entweder die [CKA](#)-Zertifizierung der Linux Foundation, eine Teilnahmebescheinigung des [LFS458-Trainings](#) oder dazu äquivalente Kenntnisse über Aufbau und Funktion von Kubernetes Clustern.

Agenda:

- Einführung in Cloud-Security-Konzepte
 - Assessment
 - Prevention
 - Detection
 - Reaction
 - Angriffsflächen und -typen
- Sichere Cluster-Konfiguration
 - Image Supply Chains
 - Policy-based Control
 - Runtime Sandbox
- Cluster-Installation
 - Updating Kubernetes
 - Kernel Hardening
- Absicherung von kube-apiserver
 - Access Restrictions
 - Role-Based Access Control
 - Auditing
 - etcd schützen
- Secure Networking
 - Netfilter-Management und -Implementierung

- Pod-to-Pod-Verschlüsselung
- Cluster Level Access beschränken

- Security und Workload
 - Workloads analysieren

 - SELinux-Grundlagen

 - AppArmor einsetzen

- Security Incidents erkennen und behandeln
 - Einführung Intrusion Detection Systems

 - Best Practices während des Vorfalls

 - Best Practices nach dem Vorfall

 - Threat Detection

 - Verhaltensanalyse