HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE-ONLINE-KURS

M 08

Offensive Kubernetes Security 101 –

ein neuer zweitägiger Live-Online-Workshop vom 07. - 08.12.2026

Lernen von den Profis – Ihre Referenten sind Sebastian Funke, Sven Nobis, Jaro Winkelhausen und Lorin Lehawany

Immer zwei der genannten Referenten halten den Kurs.

Kursbeschreibung

Container, Microservices, Kubernetes, GitOps - all diese Begriffe dominieren die modernen Softwareentwicklungsteams und -prozesse. Im ersten Teil dieses Kurses lernen Sie die technologischen Grundlagen hinter all diesen Begriffen kennen. Im zweiten Teil nehmen Sie die Perspektive eines Sicherheitsprüfers und schließlich eines Angreifers ein und lernen, einen verwalteten Kubernetes-Cluster anzugreifen und zu verteidigen. Unter anderem erhalten Sie Antworten auf die folgenden Fragen:

- Wie überprüft man die Sicherheit eines Kubernetes-Clusters?

- Wie kompromittiert man einen Kubernetes-Cluster?

Alle Themen werden durch praktische Übungen in einem geteilten Kubernetes-Cluster (K3S) begleitet und demonstriert. Am Ende dieses Workshops werden die Teilnehmer ein tiefes Verständnis für das Absichern und Angreifen von Kubernetes-Clustern sowie die Auswirkungen von Fehlkonfigurationen auf die bereitgestellten Anwendungsarchitekturen und den Betrieb einer modernen Microservice-Infrastruktur erlangt haben. Der Workshop endet mit einem Angriffs- und Verteidigungsspiel, bei dem die Teilnehmer andere Teilnehmer angreifen und sich selbst verteidigen, indem sie ihr im Laufe des Workshops erworbenes Wissen anwenden.

Offensive Kubernetes Security 101

07. - 08.12.2026 - Live Online

Diese Veranstaltung wird als Weiterbildung bei Rezertifizierungsmaßnahmen von verschiedenen Instituten anerkannt.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

Offensive Kubernetes Security 101 - ein zweitägiger Live-Online-Workshop

M 08

Kurs Agenda:

Tag 1: Einführung in Container, CI/CD, GitOps und Kubernetes sowie Kubernetes-Authentifizierung, -Autorisierung und Netzwerksicherheit

Cloud-native Plattformdienste wie GitLab, Harbor Container Registry, ArgoCD und Kubernetes (K3s) bilden heute die Grundlage moderner Softwareentwicklung und beschleunigen agile Entwicklungs- und CI/CD-Prozesse. Anwendungen können dadurch automatisiert, reproduzierbar und skalierbar bereitgestellt werden.

Nach einer kompakten Einführung in die Grundlagen von CI/CD, GitOps, Docker und Kubernetes wechseln wir direkt in unsere Laborumgebung (Coder und K3s in der Hetzner Cloud).

Anhand dieser Plattform bauen wir Container-Images, verwalten Infrastruktur deklarativ mit GitOps und deployen sowie betreiben Anwendungen in einem gemeinsam genutzten Kubernetes-Cluster.

Anschließend beschäftigen wir uns mit den Authentifizierungs- und Autorisierungsmechanismen von Kubernetes. Dabei lernen wir Best Practices, typische Fallstricke sowie Methoden zur Analyse von Role-Based Access Control (RBAC)-Konfigurationen kennen, um als Auditor Privilegieneskalationspfade systematisch zu identifizieren.

Zum Abschluss widmen wir uns der Kubernetes-Netzwerksicherheit. Wir untersuchen, wie Dienste unbeabsichtigt innerhalb oder außerhalb des Clusters exponiert werden können, wie Angreifer diese für Lateral Movement ausnutzen und wie sich die Kommunikation mithilfe von CNI-Konfigurationen und Kubernetes Network Policies wirksam absichern lässt.

Tag 2: Pod Security, Admission Controls, Secret- und Patch-Management sowie Miskonfigurationen in Kubernetes

Am zweiten Tag tauchen wir tief in die Härtung von Linux-Containern und Kubernetes Pods ein. Wir analysieren, unter welchen Voraussetzungen Angreifer aus Containern ausbrechen können, und lernen, wie sich diese Risiken systematisch auditieren und durch geeignete Sicherheitsmaßnahmen minimieren lassen.

Anschließend beschäftigen wir uns mit Sicherheitsrichtlinien und Admission Controls zur Durchsetzung von Härtungsstandards und zur sicheren Isolation von Multi-Tenant-Umgebungen.

Darauf aufbauend betrachten wir die Absicherung operativer Kubernetes-Prozesse, darunter Monitoring, Logging, Secret Management, Patch Management und Governance.

Im letzten Abschnitt analysieren wir typische Miskonfigurationen auf Control-Plane- und Data-Plane-Ebene, insbesondere in Managed-Kubernetes-Angeboten der großen Cloud-Anbieter.

Den Workshop schließen wir mit einer Attack-&-Defend-Challenge ab. Ziel ist es, den bereitgestellten Kubernetes-Cluster und den zugehörigen Cloud-Account entweder erfolgreich zu kompromittieren oder – je nach Perspektive – durch geeignete Maßnahmen wirksam gegen Angriffe zu härten.

© 2026 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.

Offensive Kubernetes Security 101 - ein zweitägiger Live-Online-Workshop

M 08

Eine Teilnahme am Workshop und den Übungen ist von jedem PC/Laptop mit stabiler Internetverbindung aus möglich. Es wird keine zusätzliche Software benötigt, ein aktueller Browser genügt (Microsoft Edge, Google Chrome oder Firefox). Das Workshopmaterial, sowie mögliche Demos und natürlich die Trainer sind stets sichtbar und werden je nach Erfordernis gezeigt bzw. hervorgehoben. Wir senden Ihnen die Kursdokumentation vor Kursbeginn und die Folien nach Kursende zu. Fragen werden direkt von den Trainern beantwortet. Mikrofon und Kamera sind optional, Sie können die Fragen auch über einen Chat stellen.

Wer sollte dieses Training besuchen und warum?

IT Sicherheitsexperten, Pentester und Auditoren mit vorhandenen K8s Vorkenntnissen, die lernen möchten, wie man ein K8s Cluster auf Sicherheitslücken und Konfigurationsschwächen untersucht.

Kubernetes Cluster Betreiber, die ihr Cluster verteidigen wollen und das Schadenspotential von Miskonfigurationen kennenlernen möchten.

Aufgrund der hohen Anzahl verfügbarer Werkzeuge und Technologien werden nicht alle Aspekte dieser im Detail beleuchtet werden können. Wir freuen uns allerdings über die Zusendung konkreter Fragen vorab, um diese in den Kurs einbauen zu können.

In jedem Fall wird ein Ansatz vermittelt, wie eine Security-Bewertung neuer/unbekannter Tools/Technologien angegangen werden kann.

Erforderliche Kenntnisse:

Die Teilnehmer sollten Erfahrung mit der Linux Kommandozeile (bash) haben und Vorerfahrung im Betrieb oder Nutzung von Container Platformen (Kubernetes).

© 2026 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.

Offensive Kubernetes Security 101 - ein zweitägiger Live-Online-Workshop

M 08

Profile der Seminarleiter:

Sebastian Funke ist ein IT Security Analyst und Researcher bei ERNW Enno Rey Netzwerke GmbH mit über 7 Jahren Expertise. Seine alltägliche Arbeit umfasst ein großes Themenfeld von Sicherheitsüberprüfungen in komplexen Unternehmenslandschaften mit Fokus auf klassischen Penetrationstests von Netzwerken, Desktop- und Webanwendungen bis hin zu Container und (Multi-)Cloud Umgebungen. In seiner Forschungszeit beschäftigt(e) er sich mit Privacy Enhancing Technologies im Internet der Dinge, Automatisierung von Sicherheitungsüberprüfungen in High-Level Cloud Umgebungen (Azure und Kubernetes), sowie der generellen Optimierung von Tools Tactics und Procedures (TTPs) in Penetrationstests. Aus akademischer Sicht hat er einen Abschluss als M.Sc. in IT-Security von der Technischen Universität Darmstadt.

Ihr Trainer, **Florian Bausch,** studierte Digitale Forensik und schrieb seine Master Thesis über die forensische Analyse von Ceph (Distributed Storage). Seit 2019 arbeitet er als Forensiker und Pentester bei der ERNW Research GmbH.

Ihr Trainer, **Sven Nobis,** arbeitet als Senior Security Analyst bei ERNW und führt dort Applikations- und Infrastruktur-Assessments durch. Er ist seit bald 20 Jahren professionell im IT-Bereich tätig und verfügt über umfassende Erfahrung mit den IT-Umgebungen unterschiedlicher Unternehmen und Konzerne. Seine Schwerpunkte liegen auf Cloud-Infrastrukturen und Red Teaming. Als ehemaliger Softwareentwickler verbindet er seine Erfahrungen aus der Softwareentwicklung und IT-Sicherheit, um komplexe Infrastrukturen tiefgreifend zu analysieren und so auch Schwachstellen und Angriffsvektoren abseits der Lehrbücher aufzudecken. Sven hat mehrere kritische Schwachstellen in Cloud-Produkten veröffentlicht, unter anderem in Produkten von Broadcom VMware sowie in verschiedenen Kubernetes-Projekten. Seine Forschungsergebnisse präsentierte er auf mehreren international renommierten IT-Sicherheitskonferenzen.

Jaro Winkelhausen arbeitet als Werkstudent bei der ERNW GmbH, wo er im Bereich Cloud Security ausgebildet wird. Derzeit absolviert er seinen Bachelor in Cybersecurity an der Technischen Hochschule Mannheim.

Lorin Lehawany arbeitet als Security Analyst bei der ERNW Enno Rey Netzwerke GmbH. Als Expertin für Cloud- und Kubernetes-Sicherheit prüft sie die Sicherheit von Infrastrukturen für zahlreiche Unternehmen in Deutschland. Darüber hinaus organisiert sie als aktives Mitglied der BlackHoodie-Community regelmäßig Veranstaltungen, um Frauen den Einstieg in die IT-Sicherheit zu erleichtern.“

Teilnehmerstimmen:

»Insgesamt wieder ein sehr gut vorbereitetes Seminar mit extrem fachkundigen Kollegen.«

Holger Haas, Brose Fahrzeugteile, Architektur und Innovation, Bamberg

© 2026 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.

Offensive Kubernetes Security 101 - ein zweitägiger Live-Online-Workshop

M 08

DETAILS ZUM ANMELDEFORMULAR

Wege zur Anmeldung

Per Post: Bitte dieses Anmeldeformular ausfüllen und an HM Training Solutions senden.

Per E-Mail: info@hm-ts.de

Per Webseite: https://www.hm-ts.de

Gebühren

2-tägiger Kurs **2.690,– €** pro Person + 19% MwSt.

Bestätigungsbrief

Ihre Anmeldung bestätigen wir per Mail oder Brief. Er enthält Details über die Veranstaltung. Der Kurspreis enthält die Seminardokumentation, Zugriff auf die Plattform sowie die Ausstellung eines Zertifikats.

Änderungen

HM Training Solutions behält sich das Recht vor, bei Eintreten nicht vorhersehbarer Umstände das Seminar räumlich und/oder zeitlich zu verlegen, einen anderen Referenten ersatzweise einzusetzen oder die Veranstaltung zu stornieren. Weitergehende Ansprüche bestehen nicht.

Stornierung seitens des Teilnehmers

Bitte reichen Sie Stornierungen schriftlich per Post oder Email (info@hm-ts.de), ein. Bestätigte Anmeldungen können bis zu sechs Wochen vor Seminarbeginn kostenfrei storniert werden, danach berechnen wir die gesamte Seminargebühr. Eine Übertragung an einen Ersatzteilnehmer ist jederzeit möglich.

Firmeninterne Seminare

Alle Trainings von HM Solutions können auch firmenintern und zugeschnitten auf den Bedarf der jeweiligen Organisation durchgeführt werden. Weitere Informationen erhalten Sie unter der Telefon-Nr. +49 (0) 6022 508 200.

Die Teilnehmerzahl ist begrenzt.
Wir berücksichtigen Ihre Anmeldung in der Reihenfolge des Eingangs.

© 2026 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.

Offensive Kubernetes Security 101 - ein zweitägiger Live-Online-Workshop

M 08

ANMELDEFORMULAR

Offensive Kubernetes Security 101

❒ **2 Tage: 07. - 08.12.2026 - live online**

❒ Bitte reservieren Sie _____ Platz/Plätze für den Kurs M 08 Offensive Kubernetes Security 101 zum oben ausgewählten live online-Termin **zum Einzelpreis von 2.690,– €** + 19% MwSt.

Herr/Frau Vorname Nachname

_____

Funktion _____

Firma _____

Adresse _____

_____

_____

Postleitzahl _____ Ort _____

Land _____

Telefonnummer _____

Mobilfunknummer _____

E-Mail _____

Unterschrift _____

Zusätzliche Teilnehmer

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Zahlung

BUCHUNGSREFERENZ HM 08

❒ Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

_____

_____

_____

PO-Nummer _____

© 2026 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.