Kubernetes – Application Developer + Cloud Native Application Security (KADCAS)

ID KADCAS **Preis** auf Anfrage **Dauer** 3 Tage

Voraussetzungen

- Basiskenntnisse der Kommandozeile unter Linux (bash, csh, zsh o.ä.)
- Erfahrung im Paketieren und Deployen von Software ist vorteilhaft
- Grundlegende Kenntnisse der Softwareentwicklung. Konkrete Technologien werden nicht vorausgesetzt.

Kursziele

Sobald der Kubernetes Cluster bereitgestellt ist (ob nun als managed Service in der Public Cloud oder on Premise durch den Betrieb) kann das DevOps Team starten, darauf Anwendungen zu deployen. Davor macht es Sinn, die Sicherheit des neuen Technologies-Stacks zu durchdenken. Wem obliegt die Verantwortung für diese? Die unterliegende Infrastruktur muss selbstverständlich durch den Betreiber abgesichert sein. Damit ist es allerdings nicht getan. Auch die Anwendungsentwicklern müssen ihren Teil zur Sicherheit beitragen. Das ist auch ohne Kubernetes und Container der Fall, jedoch bringen die neuen Abstraktionen neue Chancen und Herausforderungen mit sich.

Die Schulung gibt einen Überblick darüber, was Entwickler generell beim Thema Security beachten sollten. Im nächsten Schritt wird dargestellt, welche Angriffsvektoren durch Container dazukommen, welche Verteidigungsmassnahmen und good Practices es gibt. Schliesslich werden die Kubernetes-Bordmittel im Bereich Security vorgestellt und anhand von Übungen gezeigt, wie diese eingesetzt werden können, um die Anwendungssicherheit zu erhöhen. Dabei zeigen sich Fallstricke und eine pragmatische good Practice in Benutzung. Dabei werden unter anderem die folgenden Fragen beantwortet:

- Was ist für den sicheren Betrieb von Anwendungen in Containern zu beachten?
- Welche Bordmittel bietet Kubernetes zum Absichern von Anwendungen?
- Sind die Standardeinstellungen in Kubernetes „secure by default“?
- Welche Fallstricke gibt es beim Absichern von Anwendungen auf Kubernetes?
- Was sind good Practices für Entwickler beim Thema Cloud Native Security?
- Was sollte im Bereich Anwendungssicherheit zusätzlich beachtet werden, wenn eine Anwendung auf Kubernetes deployt wird?
- Welche Tools unterstützen uns beim Thema Sicherheit mit Kubernetes?
- Was ist beim Design von Anwendungen in Containern im Bereich Security wichtig?
- Ist die Anwendung im Container mehr oder weniger isoliert als in einer virtuellen Maschine?

Hinweis: Da Kubernetes auf Containern basiert, werden zu Begin der Schulung die wichtigsten Aspekte von Docker© Technologien aufgefrischt. Ein grundlegendes Verständnis von Container-Technologie ist jedoch erforderlich. Die Schulungsinhalte sind unabhängig von speziellen Programmiersprachen ausgelegt.

Kursinhalt

Tag1

- Auffrischung Docker© Container & Technologien
- Kubernetes-Cluster Grundlagen
- Building Blocks von Kubernetes
- Benutzung eines Managed Kubernetes Clusters
- Zugriff auf Kubernetes per Command Line Interface (kubectl)
- Pods

Tag2

- Services, Service Discovery & Loadbalancing
- Zero Downtime Deployments
- Horizontale Skalierung / Replikation
- Storage (Persistent Volumes/Persistent Volume Claims)
- State (Stateful Sets)
- Namespaces
- Weiterführende Themen für die tägliche Arbeit

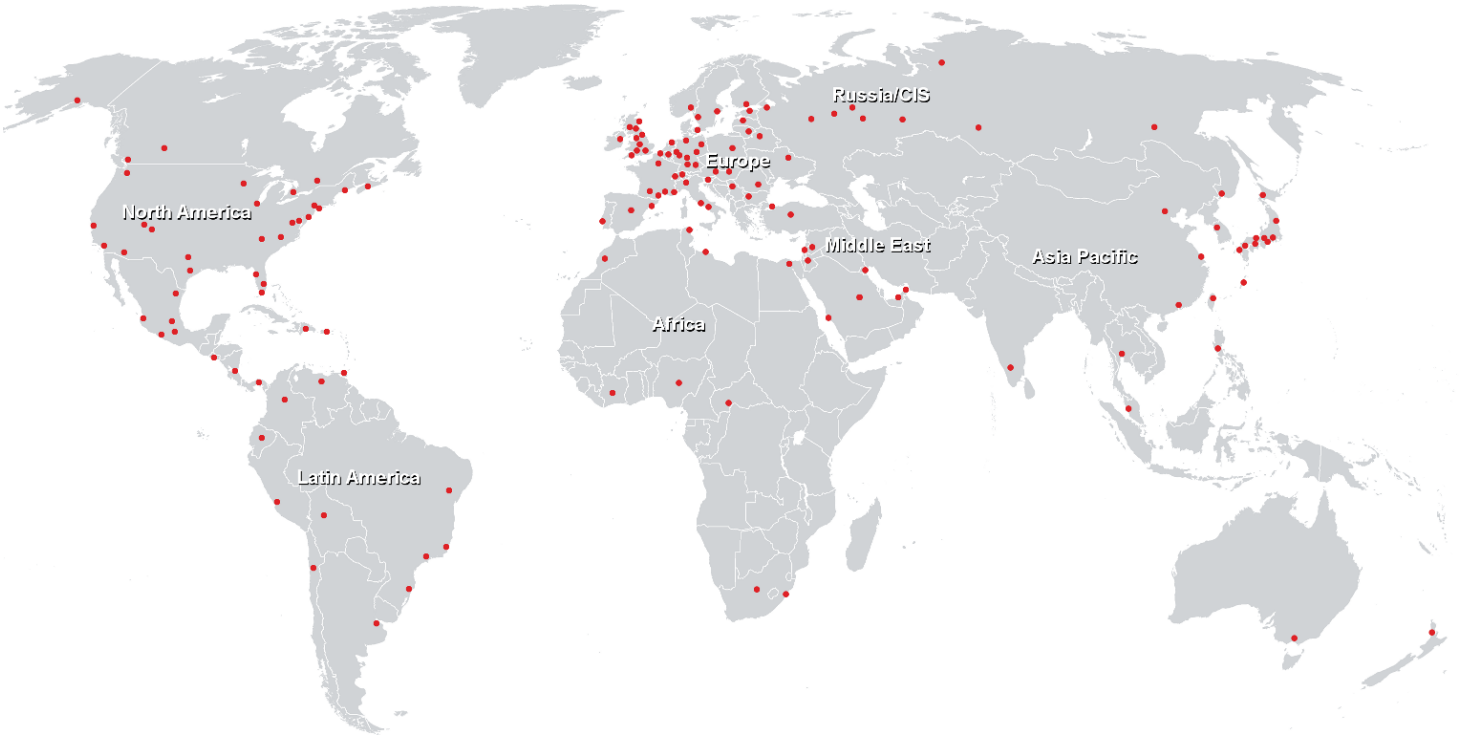
Tag3

Kubernetes – Application Developer + Cloud Native Application Security (KADCAS)

- Grundlagen Application Security
- Security Context
- Role Based Access Control (RBAC)
- Pod Security Policies
- Network Policies
- Fortgeschrittene Security Themen: Security-Mechanismen des Linux Kernels, Sandboxed Container Runtimes

Kubernetes – Application Developer + Cloud Native Application Security (KADCAS)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch