Red Hat Security: Securing Containers and OpenShift («DO425»)

Dieser Kurs unterstützt Infrastrukturadministratoren und Sicherheitsprofis dabei, Bedrohungen in der containerbasierten OpenShift-Infrastruktur zu identifizieren und zu reduzieren.

Dauer: 4 Tage
Preis: 3'400.– zzgl. 8.1% MWST

Inhalt

Der Lehrplan des Kurses *Red Hat Security: Securing Containers and OpenShift (DO425)* umfasst die Implementierung und Verwaltung sicherer Architekturen, Richtlinien und Verfahren für moderne containerisierte Anwendungen und software-definiertes Networking.

Sie lernen sichere und vertrauenswürdige Container-Images, Registries und Quellcode-Inhalte zu verwenden, Netzwerk- und Storage-Isolierung zu verwalten, Single Sign-on für Anwendungen zu implementieren sowie geeignete Sicherheitsbeschränkungen und rollenbasierte Zugriffskontrolle für Services zu konfigurieren. Dazu erfahren Sie, wie Sie mit aktuellen Linux-Kerntechnologien (darunter namespaces, Cgroups, seccomp, capabilities und SELinux) eine robuste und ausgereifte Hosting-Umgebung mit hochsicheren Containern bereitstellen.

Kursinhalt:

Beschreibung von Host-Sicherheitstechnologien

- Mehr über die Kerntechnologien erfahren, die Red Hat Enterprise Linux zu einem robusten und vertrauenswürdigen Container-Host machen

Bereitstellung vertrauenswürdiger Container-Images

- Registries, Services und Methoden des Red Hat Image-Ökosystems beschreiben

Implementierung von Sicherheit in den Build-Prozess

- Automatisierte Methoden zur Integration von Sicherheitsprüfungen in Build und Bereitstellungs-Pipelines erlernen

Management der Nutzer-Zugriffskontrolle

- Methoden zur Integration und Verwaltung der Benutzerauthentifizierung für Bediener und Webapplikationen anwenden

Kontrolle der Bereitstellungs-Umgebung

- Festlegen, wie eine Container-Plattform den Bereitstellungsprozess mithilfe von Richtlinien und Automatisierung sichert

Management einer sicheren Plattform-Orchestrierung

- Untersuchen, wie eine Container-Plattform den Orchestrierungsprozess mithilfe von Richtlinien und Infrastruktur sichert

Bereitstellung eines sicheren Netzwerk I/O

- Technologien und Kontrollfunktionen erkunden, die Mandantenfähigkeit und Projektisolierung ermöglichen

- Verschiedene Technologien und Kontrollfunktionen anwenden, die einen autorisierten, mandantenfähigen Storage-Zugriff ermöglichen

Hinweis: Aufgrund technischer Fortschritte und entsprechender Veränderungen bei den zugrundeliegenden Jobs, kann der Kursinhalt variieren.

Key Learnings

- Einführung in die Linux Mehrmandanten-Isolierung und Least-Privilege-Technologien
- Untersuchung vertrauenswürdiger Repositorys sowie Signieren und Scannen von Images
- Implementierung der Sicherheit in einer CI-/CD-Pipeline (Continuous Integration/Continuous Development)
- Integration eines Single Sign-on für Webanwendungen
- Automatisierung richtlinienbasierter Bereitstellungen
- SCC-Konfiguration (Security Context Constraint)
- Management der API-Zugriffskontrolle
- Bereitstellung eines sicheren Netzwerk I/O
- Bereitstellung eines sicheren Storage I/O

Methodik & Didaktik

Container und Container-Orchestrierungsplattformen, wie OpenShift und Kubernetes, sind mittlerweile fester Bestandteil des Unternehmens-Computings. Container-Umgebungen bringen aber auch neue Angriffsvektoren, Exploits sowie Schwachstellen mit sich. Unternehmen benötigen robuste Sicherheitseinstellungen, allerdings haben sich traditionelle Modelle der netzwerkbasierten Sicherheit für eine Migration zu containerisierten Microservices als nicht geeignet erwiesen. Entwickler müssen sicherstellen, dass Ihr Code sowie Ihre Images und Bereitstellungen vertrauenswürdig und sicher sind.

In diesem Kurs erlernen Sie die Fähigkeiten, die Sie brauchen, um in der sich ständig weiterentwickelnden Welt containerisierter Anwendungen und OpenShift-Installationen ein hohes Sicherheitsniveau aufrechtzuerhalten. OpenShift ist eine unternehmensfähige containerbasierte Anwendungsplattform, die neben der ausgereiften Sicherheitsarchitektur von Red Hat Enterprise Linux Folgendes bietet: zusätzliche Sicherheitsmechanismen für eine Zugriffskontrolle nach Servicerolle, Hardening des Build-Prozesses, Mehrschichtsicherheit mit Source Images und kontrolliertes Implementierungsmanagement. Mit diesen Features kann Ihr Unternehmen Sicherheitsverletzungen effizient reduzieren, die Geschäftsunterbrechungen, Markenerosion, einen Verlust des Kunden- und Aktionärsvertrauens sowie hohe Kosten für eine nachträgliche Problembehebung verursachen. Zudem können Sie die in diesem Kurs vorgestellten Tools dazu verwenden, um zu demonstrieren, dass die von Kunden, Betriebsprüfern oder anderen Stakeholdern festgelegten Compliance-Anforderungen eingehalten wurden.

Zielpublikum

Dieser Kurs ist für Profis gedacht, die für die Konzipierung, Implementierung, Wartung und Verwaltung der Sicherheit in containerisierten Anwendungen auf Red Hat Enterprise Linux Systemen und Red Hat OpenShift Container Platform Installationen zuständig sind und unter anderem folgende Rollen innehaben:

- Systemadministrator
- IT-Sicherheitsadministrator
- IT-Sicherheitsingenieur
- DevOps-Ingenieur
- Cloud-Entwickler
- Cloud-Architekt

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-it-provider/red-hat/red-hat-openshift/kurs-red-hat-security-securing-containers-and-openshift