EC-Council Certified DevSecOps Engineer (ECDE)

ID ECDE **Preis** CHF 3'300.– (exkl. MwSt.) **Dauer** 3 Tage

Zielgruppe

- C|ASE-zertifizierte Fachleute
- Fachleute für Anwendungssicherheit
- DevOps-Ingenieure
- Software-Ingenieure und -Tester
- IT-Sicherheitsexperten
- Cybersecurity-Ingenieure und -Analysten
- Jeder mit Vorkenntnissen im Bereich Anwendungssicherheit, der seine Karriere im Bereich DevSecOps ausbauen möchte

Voraussetzungen

Die Teilnehmer sollten ein Verständnis für Konzepte der Anwendungssicherheit haben.

Kursziele

- Verstehen Sie DevOps-Sicherheitsengpässe und erfahren Sie, wie die Kultur, Philosophie, Praktiken und Tools von DevSecOps die Zusammenarbeit und Kommunikation zwischen Entwicklungs- und Betriebsteams verbessern können.
- Verstehen Sie die DevSecOps-Toolchain und wie Sie Sicherheitskontrollen in automatisierte DevOps-Pipelines integrieren können.
- Integration von Eclipse und GitHub mit Jenkins zur Erstellung von Anwendungen.
- Richten Sie Sicherheitspraktiken wie die Erfassung von Sicherheitsanforderungen, die Modellierung von Bedrohungen und die Überprüfung von sicherem Code an den Entwicklungsabläufen aus.
- Integrieren Sie Tools zur Bedrohungsmodellierung wie Threat Dragon, ThreatModeler und Threatspec, verwalten Sie Sicherheitsanforderungen mit Jira und Confluence, und nutzen Sie Jenkins, um eine sichere CI/CD-Pipeline zu erstellen.
- Verstehen und Implementieren kontinuierlicher Sicherheitstests mit statischen, dynamischen und interaktiven Anwendungstests und SCA-Tools (z. B. Snyk, SonarQube, StackHawk, Checkmarx SAST, Debricked, WhiteSource Bolt).
- Integrieren Sie Tools zum Selbstschutz von Laufzeitanwendungen wie Hdiv, Sqreen und Dynatrace, die Anwendungen während der Laufzeit mit weniger Fehlalarmen schützen und bekannte Schwachstellen beheben.
- Integrieren Sie SonarLint in die IDEs Eclipse und Visual Studio Code.
- Implementieren Sie Werkzeuge wie das JFrog IDE Plugin und die Codacy-Plattform.
- Integrieren Sie automatisierte Sicherheitstests in eine CI/CD-Pipeline mit Amazon CloudWatch, Amazon Elastic Container Registry und AWS CodeCommit, CodeBuild, CodePipeline, Lambda und Security Hub.
- Implementierung verschiedener Automatisierungstools und -verfahren, einschliesslich Jenkins, Bamboo, TeamCity und Gradle.
- Führen Sie kontinuierliche Schwachstellen-Scans für Daten und Produkt-Builds mit automatisierten Tools wie Nessus, SonarCloud, Amazon Macie und Probely durch.
- Implementierung von Penetrationstest-Tools wie gitGraber und GitMiner zur Sicherung von CI/CD-Pipelines.
- Verwenden Sie AWS- und Azure-Tools zur Sicherung von Anwendungen.
- Integrieren Sie automatisierte Tools, um Sicherheitsfehlkonfigurationen zu erkennen, die sensible Informationen preisgeben und zu Angriffen führen könnten.
- Verstehen des Konzepts "Infrastruktur als Code" und Bereitstellen und Konfigurieren der Infrastruktur mit Tools wie Ansible, Puppet und Chef.
- Überprüfen Sie Code-Pushes, Pipelines und Compliance mithilfe von Protokollierungs- und Überwachungstools wie Sumo Logic, Datadog, Splunk, dem ELK-Stack und Nagios.
- Verwenden Sie automatisierte Überwachungs- und Alarmierungs-Tools (z. B. Splunk, Azure Monitor, Nagios) und erstellen Sie ein Echtzeit-Warn- und Kontrollsystem.
- Integrieren Sie Compliance-as-code-Tools wie Cloud Custodian und das DevSec-Framework, um sicherzustellen, dass die regulatorischen oder Compliance-Anforderungen des Unternehmens erfüllt werden, ohne die Produktion zu behindern.
- Scannen und Sichern der Infrastruktur mithilfe von Container- und Image-Scannern (Trivy und Qualys) sowie Infrastruktur-Sicherheitsscannern (Bridgecrew und Checkov).
- Integration von Tools und Praktiken zum Aufbau eines kontinuierlichen Feedbacks in die DevSecOps-Pipeline mithilfe von Jenkins und E-Mail-Benachrichtigungen von Microsoft Teams.

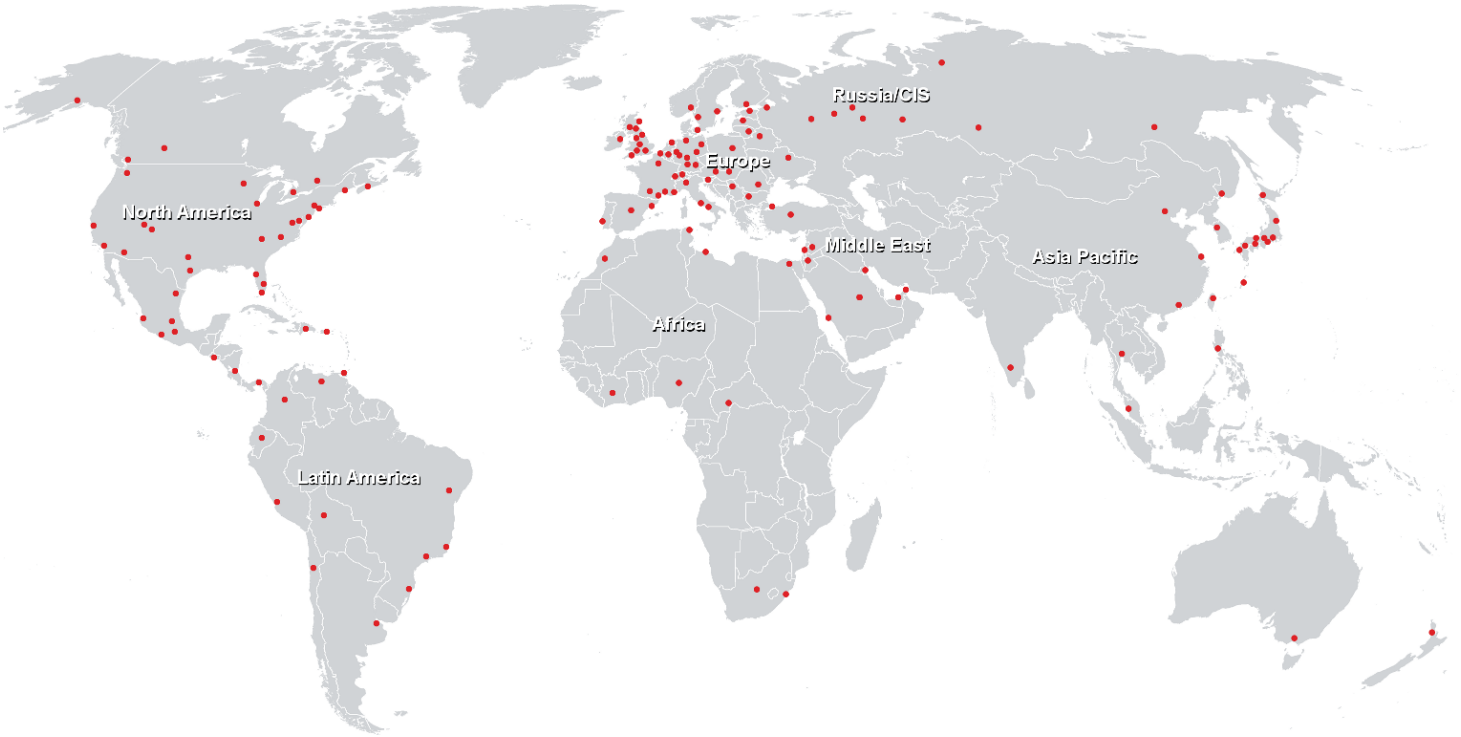
- Integrieren Sie Alerting-Tools wie Opsgenie mit Protokollmanagement- und Überwachungstools, um die Betriebsleistung und Sicherheit zu verbessern.

Kursinhalt

- Verständnis der DevOps-Kultur
- Einführung in DevSecOps
- DevSecOps-Pipeline - Planungsphase
- DevSecOps-Pipeline - Code-Phase
- DevSecOps-Pipeline - Erstellungs- und Testphase
- DevSecOps-Pipeline - Freigabe- und Bereitstellungsphase
- DevSecOps-Pipeline - Phase Betrieb und Überwachung

EC-Council Certified DevSecOps Engineer (ECDE)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

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

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