CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

Cloud 223:

Identifying Risks in Your Cloud Environment with CSPM

Course Overview:

Security in the cloud works very much the same as security in an on-premises data center. But once your cloud infrastructure is built, how do you secure it? CLOUD 223: Identifying Risks in Your Cloud Environment with CSPM will teach you how to use CrowdStrike's cloud security posture management (CSPM) module to secure your cloud environment configurations and remain in compliance with industry standards.

Find out how CSPM can help you determine if any of your cloud assets are misconfigured, if you are meeting industry standards for security and if any behaviors affecting your cloud assets are malicious. During this course, you will locate cloud accounts with vulnerabilities, find the steps to remediate them and learn where to communicate those findings.

What You Will Learn:

- Identify issues in the cloud environment related to misconfigurations, adversary behaviors, access and compliance
- Access and share the steps to remediate cloud configuration issues
- Manage workflows and policies to facilitate a fast response to cloud issues

1-day program | 2 credits

This instructor-led course includes a CSPM walkthrough and hands-on learner exercises. You will practice finding cloud configuration and behavior issues as well as the steps to remediate them.

Take this class if you are:
A cloud security administrator, a cloud security architect or studying for the CrowdStrike Certified Cloud Specialist (CCCS) exam.

Registration
For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires two (2) training credits. If you do not have access to CrowdStrike University, need to purchase training credits or need more information, please contact **sales@crowdstrike.com**

Prerequisites

- Knowledge of computer networking concepts and protocols and network security methodologies
- Basic knowledge of cloud security and the terms that different cloud providers use
- Completion of CLOUD 100: Falcon Cloud Security Fundamentals
- Completion of FALCON 114: Falcon Fusion Fundamentals
- Familiarity with administrative functions of the CrowdStrike Falcon® platform is recommended

Requirements

- Broadband internet connection, web browser, microphone and speakers
- Dual monitors and headset are recommended

Class Material

Associated materials may be accessed from CrowdStrike University on the day of class.

Topics

Cloud Security in the Falcon Platform

- Explain how a cloud-native application protection platform (CNAPP) protects a cloud environment from breaches
- Describe what a CSPM platform does
- Determine which CrowdStrike Falcon® Cloud Security roles have read and write access to CSPM pages

Indicator of Misconfiguration (IOM) Findings

- Evaluate cloud security controls and configurations to identify misconfigurations, vulnerabilities and high-risk practices
- Compare cloud configurations to the latest industry benchmarks to determine compliance
- Locate recommended remediation steps for findings related to cloud misconfigurations

Indicator of Attack (IOA) Findings

- Identify the extent of a cloud compromise, including compromised users and persistence mechanisms
- Locate recommended remediation steps for findings related to potential adversary behavior

Cloud Identity Analyzer

- Analyze and interpret identity-related findings
- Locate recommended remediation steps for findings related to identity and access issues

Public Cloud Inventory

- Organize cloud assets to monitor and investigate
- Find public-facing assets with misconfigurations
- Find assets that are connected to misconfigured assets to see if they have been affected
- Locate recommended remediation steps for findings related to public cloud inventory issues

Operationalizing CSPM

- Modify default CSPM policies
- Determine related compliance for each CSPM policy
- Recall the steps to create a custom policy or compliance
- Configure CrowdStrike Falcon® Fusion SOAR workflows to notify individuals about cloud-related policies, detections and incidents

CROWDSTRIKE
UNIVERSITY