

CLOUD 223:

Identifying and Managing Risks in Your Cloud Environment with Falcon Cloud Security

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 and Managing Risks in Your Cloud Environment with Falcon Cloud Security* utilizes CrowdStrike Falcon® Cloud Security to systematically identify, assess, prioritize, and remediate security risks across multi-cloud environments.

Find out how Falcon Cloud Security can help you determine if any of your cloud assets are misconfigured and if any behaviors affecting your cloud assets are malicious. During this course, you will locate cloud accounts with misconfigurations, find the steps to remediate them, and learn where to communicate those findings.

What You Will Learn:

In this course, you will learn how to:

- » Identify issues in cloud environments related to misconfigurations, adversary behaviors, and access
- » Locate and share the steps to remediate cloud configuration issues
- » Investigate workflow efficiencies to reduce cloud risks

1-day program | 2 credits

This instructor-led course includes hands-on labs that allow you to practice and apply what you've learned

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.

Recommended 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
- » Recommended courses:
 - » **CLOUD 100:** Falcon Cloud Security Fundamentals
 - » **FALCON 200:** Falcon Platform for Administrators or familiarity with the administrative functions of the CrowdStrike Falcon® platform

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

Viewing and Managing Cloud Assets

- » Navigate the Cloud Assets Dashboard to gain high-level visibility into multi-cloud asset inventory
- » Use the Assets Explorer to inventory, search, and organize cloud assets while identifying anomalies
- » Explore asset graphs to visualize risk relationships and attack paths for enhanced security investigations

Cloud Security in Falcon

- » Determine how Falcon Cloud Security gathers cloud posture data across cloud environments
- » Use Falcon Cloud Security to monitor cloud environments for risks and misconfigurations
- » Evaluate Falcon Cloud Security's continuous compliance monitoring across frameworks and integration of compliance with broader security activities
- » Implement data security posture management (DSPM) controls to protect sensitive information

Detecting and Responding to Misconfigurations

- » Examine different types of cloud misconfigurations (network, storage, compute, identity, encryption) and assess their security implications
- » Evaluate indicator of misconfiguration (IOM) severity levels and risk scoring methodologies to correlate security findings with business impact
- » Implement suppression rules and technical remediation procedures for cloud security misconfigurations

Identifying and Responding to Indicators of Attack (IOAs)

- » Identify suspicious behaviors that trigger IOA alerts to detect potential attack activities
- » Determine appropriate incident response procedures based on Falcon Cloud Security IOA findings to contain and remediate threats

Managing Cloud Risks

- » Differentiate between detection, investigation, and risk management activities to establish comprehensive security workflows
- » Interpret risk context indicators to prioritize security actions based on business impact
- » Identify appropriate next steps for cloud risk management workflows that align security operations with business objectives

