CrowdStrike University

CLOUD 271
SECURING CLOUD WORKLOADS AND CONTAINERS WITH FALCON CLOUD SECURITY

COURSE OVERVIEW

The complexity of public and private cloud infrastructure requires development teams to incorporate security into all aspects of the development lifecycle. In *CLOUD 271: Securing Cloud Workloads and Containers with Falcon Cloud Security*, you will learn to use CrowdStrike Falcon® Cloud Security and “shift left” to protect containerized workloads and cloud-native applications.

This course includes security best practices and tips for using Falcon Cloud Security to mitigate common threats to cloud workloads. You will learn to proactively identify common threats and mitigate risks at every stage of application development. Learn how to avoid the financial and reputational costs of breaches to your organization, as well as improve your overall security posture.

WHAT YOU WILL LEARN

- Determine which sensor and agent deployment options work best for your environment
- Identify risky configurations and behaviors to secure cloud-native applications and containers during the whole development lifecycle
- Implement security best practices in a DevSecOps environment

PREREQUISITES

- Basic knowledge of cloud computing and related terms like containers, workloads, instances, buckets and Kubernetes cluster
- Familiarity with at least one cloud provider (AWS, Azure, GCP)
- Completion of CLOUD 100: Falcon Cloud Security Fundamentals
- Completion of CLOUD 172: Setting Up Cloud Workload Protection with Falcon Cloud Security

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.

1-day program | 2 credits

This course will cover security best practices for DevSecOps methodologies and provide practical, hands-on experience using Falcon Cloud Security to find pre-runtime and runtime issues in a development lifecycle.

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.

KUBERNETES AND CONTAINERS OVERVIEW

- Explain how Falcon container security can protect an environment during the software development lifecycle
- Gain familiarity with the Kubernetes and Containers dashboard in the Falcon platform
- Recall the roles that can have access and can perform tasks for container security in the Falcon platform

SENSOR DEPLOYMENT

- Recall the different deployment options for container security with Falcon
- Use a compatibility flowchart to determine which deployment options work for a particular environment

KUBERNETES PROTECTION

- Identify high-level trends, hierarchies and misconfigurations in your Kubernetes environment
- Identify asset metrics for containers and their running status, pod details and cluster details for multiple cloud providers under one pane of glass
- Identify issues with Kubernetes deployments across different cloud service providers and self-managed environments
- Create Admission Controller policies to take action or alert on indicators of misconfiguration in the Kubernetes environment

RUNTIME PROTECTION

- Recall common issues that occur during runtime
- Explain the detection and prevention policy options for Falcon container security
- Identify where to find common runtime issues using the Falcon platform
- Review a detection for drift indicators and find a suggested remediation

IMAGE REGISTRIES AND ASSESSMENTS

- Describe how image assessment with Falcon Cloud Security helps organizations to "shift left"
- Explain the differences between the three methods for image assessment with Falcon
- Recall the different registries currently supported by Falcon Coud Security
- Explain how to connect a supported image registry
- Find issues with registry connections using the Falcon platform

REVIEWING IMAGES

- Recall common pre-runtime issues in the software development lifecycle
- Identify common pre-runtime issues using the Falcon platform
- Review a vulnerable image and find a suggested remediation
- Create image assessment policies to prevent pre-runtime issues