CLOUD 271: Securing a Runtime Environment with Falcon Cloud Security

OEM: CrowdStrike • Code: CLOUD 271

COURSE DESCRIPTION

Your containers aren't just at risk during build or deployment — the real battle happens at runtime. In CLOUD 271: Securing a Runtime Environment with Falcon Cloud Security, you will learn how to use CrowdStrike Falcon® Cloud Security to gain the visibility and control needed to secure containers at runtime — where the real action is. You will learn to proactively identify common runtime threats with agents like the Kubernetes Admission Controller (KAC), Image Assessment at Runtime (IAR), and the CrowdStrike Falcon® sensor or Falcon container sensor for Linux. You will also learn to mitigate risks at runtime with KAC, image assessment, and prevention policies. This course includes security best practices and tips for using Falcon Cloud Security to mitigate common runtime threats to cloud workloads and improve your overall runtime security posture.

AUDIENCE PROFILE

- This class is best suited for roles that identify cloud security risks and vulnerabilities with the Falcon platform, update cloud security policies, and communicate findings to technical teams (incident responders, developers, DevOps), including:
- Cloud security administrator
- Cloud security analyst
- Cloud risk manager
- People preparing for the CrowdStrike Certified Cloud Specialist (CCCS) exam

PREREQUISITES

- Fundamental knowledge of cloud computing and related terms like containers, workloads, instances, buckets, and Kubernetes clusters
- Familiarity with at least one cloud provider (AWS, Azure, Google Cloud)

Recommended courses:

  - CLOUD 100: Falcon Cloud Security Fundamentals
  - FALCON 200: Falcon Platform for Administrators
- Broadband internet connection, web browser, microphone and speakers
- Dual monitors and headset are recommended

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- Identify risky Kubernetes configurations with KAC
- Identify risky behaviors in a runtime environment with the Falcon sensor
- Configure KAC and image assessment policies that prevent risky containers from deploying to runtime
- Configure prevention policies that alert on and block risky processes from running in your container workloads

COURSE OUTLINE

Module 1: Introduction to CrowdStrike's Runtime Security

- Recall the threats that can occur in a runtime environment
- Explain how Falcon Cloud Security protects runtime environments with tools like the Falcon sensor, KAC, and IAR
- Identify details for the sensors and agents installed in a runtime environment on the Host Management page in the Falcon platform
- Identify runtime issues from a sample container workload environment in the Falcon platform

Module 2: Using KAC for Visibility

- Explain how KAC helps protect a runtime environment
- View details about objects running in your Kubernetes environment using the Falcon console
- Find running containers and images that are not protected by KAC, IAR, or the Falcon sensor

Module 3: Preventing Risky Kubernetes Deployments

- Identify misconfigurations in your Kubernetes environment using the Falcon platform
- Find recommended remediations for KAC misconfigurations
- Recommend KAC and image assessment policy configurations that alert on or prevent Kubernetes misconfigurations and image vulnerabilities

Module 4: Using Prevention Policies for Runtime Protection

- Analyze a sample cloud detection in the Falcon platform to assess risk severity, determine appropriate response teams (security vs. development), and recommend actions
- Suggest prevention policy configurations that match the recommendations found in Falcon support documentation