SIEM 211: Incident Response and Investigation in Falcon Next-Gen SIEM

OEM: CrowdStrike • Code: SIEM 211

COURSE DESCRIPTION

Transform your security operations using CrowdStrike Falcon® Next-Gen SIEM. In this comprehensive course for security analysts, investigators, security operations specialists, and security leads, you'll get hands-on experience in investigating third-party data in Falcon Next-Gen SIEM, building and managing cases, correlating events, and monitoring and analyzing third-party data. You'll learn the skills to actively investigate incidents and identify potential threats and vulnerabilities within an organization's network. By utilizing Falcon Next-Gen SIEM, you'll adopt a comprehensive approach to security monitoring, analyzing environmental data, and correlating events to provide additional context. This will enable you to uncover hidden threats or indicators of compromise (IOCs) that traditional security controls might overlook. And, you'll develop expertise in threat hunting, continuous monitoring, and advanced threat detection using Falcon Next-Gen SIEM tools, empowering you to safeguard your organization against evolving cyber threats.

AUDIENCE PROFILE

- an incident responder, global SOC analyst, Falcon Next-Gen SIEM analyst, security lead, or customer that has purchased CrowdStrike Falcon® Insight XDR or Falcon Next-Gen SIEM

PREREQUISITES

- CQL 101: CrowdStrike Query Language Fundamentals 1
- CQL 102: CrowdStrike Query Language Fundamentals 2
- CQL 201: Designing and Optimizing CQL Queries
- FALCON 201: Falcon Platform for Responders
- SIEM 100: Next-Gen SIEM Fundamentals
- SIEM 106: Case Management Fundamentals
- 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:

- Leverage Falcon Next-Gen SIEM for analysis and response
- Apply a comprehensive approach to security monitoring by continuously analyzing Falcon Next-Gen SIEM data for potential threats, vulnerabilities, and IOCs

- Create and manage Falcon Next-Gen SIEM dashboards to identify trends and patterns
- Manage an investigation from detection through closure within the Falcon Next-Gen SIEM case management structure

COURSE OUTLINE

Module 1: Next-Gen SIEM Navigation

- Navigate the Falcon Next-Gen SIEM module and its sections
- Identify the core components of the case-centric workflow

Module 2: Managing and Analyzing Data

- Explain the roles of detections, entities, events, and cases
- Describe the CrowdStrike Parsing Standard (CPS) for ingested data
- Determine the original source of different event data
- Apply the necessary steps to investigate an initial detection in Falcon Next-Gen SIEM

Module 3: Case Management for Analysts

- Summarize the fundamentals of security case management
- Describe the phases of the Case Workflow and its elements
- Understand and apply Case Templates to define SLAs, workflow triggers, and escalation paths
- Add evidence to and collaborate on a case
- Follow a 6-step analytical process for investigation

Module 4: Advanced Event Search

- Understand the basic concepts of CrowdStrike Query Language (CQL)
- Utilize query functions such as filtering and aggregation
- Create and manage saved and parameterized searches
- Leverage saved searches as part of a broader security investigation
- Visualize event data to find hidden threats and IOCs

Module 5: Rules

- Explain the purpose and fundamentals of correlation rules
- Create, edit, and delete correlation rules
- Tune and troubleshoot correlation rules

Module 6: Dashboards

- Create a custom dashboard and add relevant widgets
- Export and import dashboards for team sharing
- Utilize data visualizations to gain security insights