CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

SIEM 212:

Investigating and Hunting Threats in Falcon Next-Gen SIEM

Course Overview:

Master CrowdStrike Falcon® Next-Gen SIEM with this targeted course for security leads, investigators, hunters, security analysts and security operations specialists. Get hands-on experience in investigating third-party data in Falcon Next-Gen SIEM, correlating events, and monitoring and analyzing third-party data.

During the course, you'll learn how to actively search for potential threats and vulnerabilities within an organization's network. You will learn to analyze historical data and correlate events and see how Falcon Next-Gen SIEM can uncover hidden threats or indicators of compromise that traditional security controls might miss. Additionally, you'll learn to establish a proactive approach to security monitoring by leveraging Falcon Next-Gen SIEM tools for proactive threat hunting, continuous monitoring and advanced threat detection, enabling you to protect your organization against evolving cyber threats.

What You Will Learn:

In this course, you will learn how to:

- Establish a proactive approach to security monitoring by continuously analyzing Falcon Next-Gen SIEM data for potential threats, vulnerabilities or indicators of compromise (IOCs)
- Review Falcon Next-Gen SIEM reports and dashboards to identify trends and patterns

1-day program | 2 credits

This instructor-led course includes various walkthrough and hands-on learner exercises

Take this class if you are:
a Falcon Platform Administrator, Falcon Next-Gen SIEM Administrator, Falcon Next-Gen SIEM Security Lead, Investigator, Hunter, Security Analyst or Security Operations Specialist

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

Version: 8.2024

Recommended Prerequisites

- Fundamental knowledge of security information and event management (SIEM) and/or log management platforms
- Intermediate knowledge of threat hunting and incident investigation
- Ability to comprehend course curriculum presented in English
- Familiarity with Microsoft Windows and Linux system logs
- Recommended courses:
  - **CQL 101:** CrowdStrike Query Language Fundamentals 1
  - **SIEM 100:** Next-Gen SIEM Fundamentals
  - **FALCON 151:** Incident Workbench Fundamentals
  - **FALCON 202:** Investigating and Querying Event Data with Falcon EDR

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

Threat Hunting in Falcon Next-Gen SIEM

- Explain investigation methodologies
- Explore threat hunting techniques in Falcon Next-Gen SIEM
- Analyze Falcon Next-Gen SIEM data for threats, vulnerabilities and IOCs

CrowdStrike Query Language (CQL) Overview

- Search for threats and vulnerabilities with CQL
- Explore the basics of CQL, including functions and aggregations

Event Search and Advanced Event Search

- Navigate to Event Search and Advanced Event Search
- Explore Advanced Event Search
- Build advanced queries
- Visualize output event data
- Create scheduled searches
- Export and report on event data

Correlation Rules

- Describe the purpose of correlation rules
- Navigate to templates provided by CrowdStrike
- Create a correlation rule
- Explain limitations and considerations
- Activate or deactivate a correlation rule
- Edit a correlation rule
- Delete a correlation rule

Event Correlation and Investigation

- Correlate different logs and events to see the bigger picture of a potential security incident
- Explore Incident Workbench

Continuous Monitoring Using Custom Dashboards

- Create your own customized dashboard widgets from a search query
- Explore widgets and data visualization options
- Leverage out-of-the-box dashboard templates
- Convert to a live dashboard
- Collaborate with the team using saved dashboards
- Export a custom dashboard to PDF

Best Practices

- Recall best practices to enhance efficiency and improve detection and response times with Falcon Next-Gen SIEM

CROWDSTRIKE UNIVERSITY