CROWDSTRIKE University

SIEM 211:

Incident Response and Investigation in Falcon Next-Gen SIEM

Course Overview:

Transform your security operations using CrowdStrike Falcon® Next-Gen SIEM in this comprehensive 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, utilizing CrowdStrike Falcon® Fusion SOAR automations, leveraging Falcon Next-Gen SIEM capabilities, and monitoring and analyzing third-party data.

In this course, you will 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. Furthermore, 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.

What You Will Learn:

In this course, you will learn how to:

- Leverage Falcon Next-Gen SIEM for incident analysis and response
- Apply a comprehensive approach to security monitoring by continuously analyzing Falcon Next-Gen SIEM data for potential threats, vulnerabilities, or IOCs
- Review Falcon Next-Gen SIEM dashboards to identify trends and patterns

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

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: 6.2025

Recommended Prerequisites

- Ability to comprehend course curriculum presented in English
- Knowledge of incident response and handling methodologies
- Recommended courses:
  - **CQL 101:** CrowdStrike Query Language Fundamentals 1
  - **FALCON 114:** Falcon Fusion SOAR Fundamentals
  - **FALCON 151:** Workbench Fundamentals
  - **FALCON 201:** Falcon Platform for Responders
  - **FALCON 202:** Investigating and Querying Event Data with Falcon EDR
  - **SIEM 100:** Next-Gen SIEM Fundamentals

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

Getting Started with Analysis in Falcon Next-Gen SIEM

- Explain CrowdStrike Falcon® platform analysis workflows
- Explore advanced investigation techniques using Falcon Next-Gen SIEM
- Analyze data for threats, vulnerabilities, and IOCs

CrowdStrike Query Language (CQL) Overview

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

Event Search and Advanced Event Search

- Explore Event Search
- Build advanced queries
- Visualize output event data
- Create scheduled searches
- Generate and export event data and reports

Correlation Rules

- Create a correlation rule using templates provided by CrowdStrike
- Activate or deactivate a correlation rule
- Edit and delete correlation rules

Event Relationship and Investigation

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

Falcon Fusion SOAR Workflows for Falcon Next-Gen SIEM Automation

- Navigate and explain the options available in the Falcon Fusion SOAR menu
- Recall the Falcon Fusion SOAR workflow creation and testing process
- Identify automation opportunities for Falcon Fusion SOAR and Falcon Next-Gen SIEM
- Troubleshoot Falcon Fusion SOAR workflows and identify potential solutions

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
- Collaborate with the team using saved dashboards
- Export a custom dashboard to PDF