CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

SIEM 211:

Incident Response in Falcon Next-Gen SIEM

Course Overview:

Leverage the power of CrowdStrike Falcon® Next-Gen SIEM in this course designed for analysts. Elevate your detection and incident workflows utilizing the full power of the expanded data and correlations offered through CrowdStrike Falcon Next-Gen SIEM.

During this course, you'll explore data correlation between the CrowdStrike Falcon® platform and third-party sources, utilize expanded datasets and Falcon Next-Gen SIEM capabilities to elevate your analysis workflows, and explore CrowdStrike Falcon® Fusion SOAR automations leveraging Falcon Next-Gen SIEM capabilities. You will also learn to identify and address connector, parser and ingest concerns from an analyst's perspective.

What You Will Learn:

By the end of this course, you will learn how to:

- Utilize Falcon Next-Gen SIEM data in analysis
- Identify and troubleshoot parsing and the data onboarding process
- Understand correlation rules
- Leverage correlated data in detection and incident analysis and response
- Work collaboratively using the Incident Workbench
- Interpret and troubleshoot Falcon Fusion SOAR workflows
- Build a simple Falcon Fusion SOAR workflow for Falcon Next-Gen SIEM

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 a 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: 8.2024

Recommended Prerequisites

- Ability to comprehend course curriculum presented in English
- Knowledge of incident response and handling methodologies
- Recommended courses:
  - **FALCON 109:** Using MITRE ATT&CK and Falcon Detection Methods to Understand Security Risk
  - **FALCON 114:** Falcon Fusion SOAR Fundamentals
  - **FALCON 115:** Create a Falcon Fusion SOAR Workflow
  - **SIEM 100:** Next-Gen SIEM Fundamentals
  - **CQL 101:** CrowdStrike Query Language Fundamentals 1
  - **FALCON 120:** Investigation Fundamentals
  - **FALCON 151:** Incident Workbench Fundamentals
  - **FALCON 201:** Falcon Platform for Responders

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 the class.

Topics

Introduction to Falcon Next-Gen SIEM and Incident Response

- Understand CrowdStrike Falcon analysis workflow
- Understand detections, incidents and associated workflows
- Explore the fundamentals of collaborative analysis

Collaborative Analysis Using Incident Workbench

- Leverage Incident Workbench for collaborative analysis
- Demonstrate collaborative analysis and response best practices and techniques

Falcon Fusion SOAR Workflows for Falcon Next-Gen SIEM Automation

- Navigate and understand the options available in the Falcon Fusion SOAR menu
- Understand 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

Understanding Falcon Next-Gen SIEM Data Onboarding

- Understand the Falcon roles and high-level Falcon Next-Gen SIEM data onboarding processes
- Troubleshoot data onboarding misconfigurations and errors
- Navigate and understand data connectors and how to ingest data into Falcon Next-Gen SIEM
- Identify the need for new data collectors and how to request them

Log Management and Correlation Rules

- Explore log management for analysis
- Identify correlation rule use cases
- Identify and troubleshoot missing or inaccurate data due to parsing or onboarding errors
- Understand the potential impact correlation rules have on your investigations

CROWDSTRIKE
UNIVERSITY