CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

SIEM 210:

Onboarding Third-Party Data and Managing Falcon Next-Gen SIEM

Course Overview:

Master CrowdStrike Falcon® Next-Gen SIEM with this targeted course for system administrators, security engineers, data custodians and data managers. Get hands-on experience in core Falcon Next-Gen SIEM functions, focusing on administration-specific tasks and performing initial setup and configuration.

During the course, you'll learn to integrate third-party data sources into the Falcon platform using the CrowdStrike Parsing Standard (CPS) and Falcon Data Connectors. Additionally, you'll learn to monitor data ingestion volumes and ensure the health and performance of your connectors, enhancing your organization's security posture and operational efficiency.

What You Will Learn:

» Learn the core functions of Falcon Next-Gen SIEM.

» Navigate the administration-specific sections of Falcon Next-Gen SIEM in the Falcon platform.

» Perform the initial configuration and setup as a Falcon Next-Gen SIEM Administrator.

» Integrate systems and connections necessary to onboard third-party data.

» Integrate custom, local and third-party data into the Falcon platform using appropriate ingest methods.

» Understand the CrowdStrike Parsing Standard for data normalization.

» Utilize out-of-the-box connectors.

» Monitor data ingestion volumes.

» Monitor the health and performance of the connectors.

1-day program | 2 credits

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

Take this class if you are:
Falcon Platform Administrator, Next-Gen SIEM Administrator, Data Manager, Security Architect, Infrastructure Support Specialist or Security Engineer/Data Custodian

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

Recommended Prerequisites

- Fundamental knowledge of SIEM and/or log management platforms
- Fundamental knowledge of preparing, ingesting and parsing log data
- Ability to comprehend course curriculum presented in English
- Familiarity with Microsoft Windows and Linux system logs
- Working knowledge of Regular Expressions
- Recommended courses:
  - **CQL 101:** CrowdStrike Query Language Fundamentals 1
  - **SIEM 100:** Next-Gen SIEM Fundamentals
  - **Falcon 200:** Falcon Platform for Administrators

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

Overview of SIEM Technology

- Identify key features of Falcon Next-Gen SIEM
- Navigate the Falcon Next-Gen SIEM menu and review key tasks for onboarding third-party data and managing Falcon Next-Gen SIEM
- Identify Falcon Next-Gen SIEM role permissions and understand their importance

Log Management

- Understand and recall log management strategies including collection, normalization, retention and disposal
- Review ingest use cases and understand supported ingest methods
- Compare and contrast the various CrowdStrike data retention subscriptions
- Understand compliance in the context of a Falcon Next-Gen SIEM Administrator

Onboarding Third-Party Data

- Recall how to get data into Falcon Next-Gen SIEM
- Review available Data Connector data sources
- Review the HEC/HTTP Event Connector
- Add and manage Data Connectors
- Use connectors to integrate and manage ingestion of third-party data sources
- Audit and monitor Data Connectors
- Align data to the CrowdStrike Parsing Standard
- Ingest data with the Falcon LogCollector

Managing and Monitoring Log Sources

- Verify data availability through querying
- Set up and fine-tune data parsers to ensure data ingestion
- Check the health of connectors
- Monitor connector metrics
- Manage connector alert settings
- Manage log source alert settings

CROWDSTRIKE
UNIVERSITY