CROWDSTRIKE University

# SIEM 210:

## Onboarding and Managing Data Sources in Falcon Next-Gen SIEM

### Course Overview:

In this course, designed for system administrators, security engineers, and data managers, learn to onboard and manage data sources in CrowdStrike Falcon® Next-Gen SIEM. Explore techniques for data source integration, connection management, and data normalization. Through hands-on exercises, onboard various data types using data connectors, implement proper data parsing using CrowdStrike Parsing Standard (CPS), and ensure reliable data flow. The course covers critical aspects of managing the data pipeline, from initial connection setup to ongoing maintenance and troubleshooting.

### What You Will Learn:

In this course, you will learn how to:

- Understand data collectors for various source types
- Create and configure data connections
- Apply CPS for data normalization
- Monitor data source health and troubleshoot common issues
- Validate data completeness and accuracy
- Apply best practices for data source management

**1-day program | 2 credits**

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

**Take this class if you are:**
a security engineer, SOC administrator, security analyst, or data engineer

**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

- 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
  - **SIEM 200:** Administering and Optimizing Next-Gen SIEM
  - **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

### Onboarding Fundamentals

- Understand data ingestion pipeline architecture
- Navigate the platform interface

### Data Connector Discovery

- Understand supported data sources and connector types
- Search and identify appropriate connectors for specific needs
- Evaluate connector capabilities and associated detection rules
- Identify beta connectors and understanding version updates

### Data Connection Configuration

- Create and configure new data connections
- Configure various log source types
- Implement connection prerequisites and best practices
- Manage existing connections effectively

## Data Source Integration

- Understand and implement event tagging
- Implement data partitioning and organization
- Configure and validate connections

## Parsing and Normalization

- Modify parsers for CPS compliance
- Configure custom field extraction rules
- Test and optimize parsing configurations
- Implement AI Parser functionality

## Data Management and Enrichment

- Create and manage lookup files
- Implement detection rules at parsing level
- Apply data enhancement techniques

## Monitoring

- Set up connection monitoring alerts
- Implement logging hygiene monitoring
- Track connection status and performance
- Validate data completeness
- Diagnose and resolve common issues