

LOG 210

Falcon LogScale Administration and Data Ingestion

Course Overview

Are you ready to elevate your skills and master CrowdStrike® Falcon LogScale™? This comprehensive course on managing and administering Falcon LogScale is designed for log managers and system administrators in security or IT. In hands-on exercises, detailed walkthroughs, and expert guidance, you'll gain the expertise to manage repositories, views, log sources, and automations efficiently. Enroll today and take the first step toward becoming a Falcon LogScale expert.

What You Will Learn

In this course, you will learn how to:

- » Identify components of the Falcon LogScale architecture
- » Recall the structure of an event, including types of fields and their purposes
- » Create and configure parsers in Falcon LogScale and explain the role of CrowdStrike Parsing Standard (CPS) to standardize and normalize events
- » Ingest data into Falcon LogScale using the Falcon LogScale Collector (FLC) and APIs
- » Manage users, groups, and roles in Falcon LogScale to control access and permissions
- » Configure and manage query auditing, special repositories, and internal monitoring in Falcon LogScale

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: a log manager/data custodian or a system administrator in a security or IT team

This course is intended for customers administering CrowdStrike-managed cloud deployments of Falcon LogScale

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

- » Completion of LOG 101: Getting Started with Falcon LogScale
- » Familiarity with log management concepts and basic understanding of regular expressions
- » Experience in managing and analyzing log files using terminal-based tools
- » A fully operational Falcon LogScale environment, as this course focuses on day-to-day administration and management rather than initial setup

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

Data Ingestion Architecture

- » Recall the components of a Repository and a View
- » Explain ingestion mechanisms in Falcon LogScale
- » Explain log ingestion through API endpoints and the Falcon LogScale Collector (FLC)
- » Use Fleet Management to deploy and administer instances of the FLS

Data Parsing

- » Recall the purpose and importance of metadata and tag fields in events
- » Parse formatted dates and times to normalize data
- » Use the CrowdStrike Parsing Standard (CPS) for normalization and standardization of data

Organization Management Essentials

- » Use permission levels to manage the organization, repositories, and assets
- » Explain how roles, groups, and users are managed within Falcon LogScale
- » Audit logs to monitor performance, organization usage, and user activity

