LOG 200:

Managing and Administering Falcon LogScale

Course Overview

Are you ready to elevate your skills and master CrowdStrike® Falcon LogScale™? Join our comprehensive Managing and Administering Falcon LogScale course designed for log managers and system administrators in security or IT. With hands-on exercises, detailed walkthroughs and expert guidance, you'll gain the expertise to manage repositories, views, collectors, dashboards and automations efficiently. Don't miss this opportunity to enhance your operational efficiency and proactive incident management skills.

Enroll today and take the first step toward becoming a Falcon LogScale expert!

Learning Objectives

- Manage repositories, views, the Falcon LogScale Collector, dashboards and automations within Falcon LogScale.
- Manage data, tokens, users and packages conforming to specific organizational needs.
- Execute day-to-day tasks inside Falcon LogScale Cloud, including managing data, integrations, access and data management architecture.

Course Length/ Cost

1-day program | 2 credits

How You Will Learn

This instructor-led course includes hands-on labs that allow you to practice and apply what you've learned.

Audience

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 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.

Prerequisites

To obtain the maximum benefit from this class, you should meet the following requirements:

- Complete ***LOG 101: Getting Started with Falcon LogScale.***
- Comprehend course curriculum presented in English.
- Have familiarity with Linux command line environments, coding languages like Python, Bash scripting and writing YAML configuration files.
- Have familiarity with log management concepts and basic understanding of regular expressions.
- Have experience managing and analyzing log files using terminal-based tools.
- Have a fully operational Falcon LogScale environment in place, as this course focuses on day-to-day administration and management rather than initial setup.

Class Material

Download the *LOG 200 Learner Guide, Lab Guide* and associated materials from CrowdStrike University once the class starts.

Course Outline

Organization Settings Essentials

- Recall key principles of Falcon LogScale's architecture.
- Recall the required permission levels to perform administrative functions within Falcon LogScale Cloud.
- Learn how Roles, Groups and Users are managed within Falcon LogScale.
- Create Roles, create Groups and assign permissions within the UI and using GraphQL.
- Assign Roles, Groups and permissions with the Repository & View Permission level.

Repository Configuration and View Management

- Identify the function and purpose of repositories and views within Falcon LogScale.
- Review the settings of repositories and views in detail to manage day-to-day operations.
- Apply Field Aliasing to rename fields for better readability and consistency at search time, improving data analysis and reporting capabilities within Falcon LogScale.
- Evaluate ingest settings, egress settings, data connections and access control, ensuring they meet organizational standards for security and efficiency.
- Build and create Event List Interactions to enrich log data.

Ingesting Data and Managing the Falcon LogScale Collector

- Recognize the various methods of data ingestion and parsing available in Falcon LogScale.
- Understand the impact of data ingestion on system performance and integrity.
- Implement data ingestion and parsing configurations.
- Analyze and optimize data ingestion workflows for improved efficiency and accuracy.
- Use Fleet Management to monitor the status of your Falcon LogScale Collector instances and configure any required enrollment token options.

Visualizations, Automations and Actions

- Use Lookup Files, Saved Queries and Dashboard Interactions and deploy Shared Wall Monitor URLs using appropriate environmental security settings.
- Create alerts, scheduled searches and actions to support environmental automation needs.
- Configure automated tasks and alerts to send webhooks and log alerts from the platform.
- Judge the effectiveness of automation rules and alert configurations in various scenarios.

Management and Auditing

- Perform package management, including importing and exporting packages.
- Review the ingress and egress controls, such as IP filters and the Amazon S3 archive.
- Audit data ingest, license usage and user activity.
- Apply technical controls to restrict certain queries within the environment.

Administrative Case Study

- Set up and configure repositories and views for data ingestion.
- Update and configure the Falcon LogScale Collector.
- Apply role-based access control (RBAC) settings and configure security measures.
- Set up automated alerts for the dataset.

CROWDSTRIKE
UNIVERSITY