CrowdStrike University

CROWDSTRIKE UNIVERSITY

LOG 201

PREPARING, INGESTING AND PARSING LOG DATA USING FALCON LOGSCALE

COURSE OVERVIEW

Does your organization use CrowdStrike® Falcon LogScale™ to aggregate and search data from a wide variety of log sources at scale? This course offers a deep dive into preparing, ingesting and parsing data sets using Falcon LogScale. Designed for those who are new to the field or looking to refresh their skills, the course presents techniques for data cleaning, dimensionality reduction, normalization and statistical interpretation. Delve into key data analysis terminology, familiarize yourself with widely used log formats and discover proven methods for data preparation. This course is especially beneficial for roles such as data analysts, IT administrators and log management specialists.

WHAT YOU WILL LEARN

In this course, you will:

- Navigate the Falcon LogScale interface.
- Create and manipulate fields to improve efficiency and accuracy of data analysis in Falcon LogScale.
- Prepare and ingest data.
- Conduct exploratory data analysis and summary statistics in a Jupyter Notebook using Python.
- Define problems and plan for a data set.
- Implement data cleaning techniques.

PREREQUISITES

- Completion of LOG 101: Getting Started with LogScale
- Ability to comprehend course curriculum presented in English
- Basic knowledge of and/or experience with Microsoft Windows and Linux environments
- Familiarity with log management concepts and regular expression usage

CLASS MATERIAL

Download your Learner Guide and Lab Guide from CrowdStrike University once the class starts.

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 data analyst, IT administrator or log management specialist. This course is intended for organizations that have purchased or are looking to purchase 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 need to purchase training credits, need more information or do not have access to CrowdStrike University, please contact sales@crowdstrike.com.

© 2023 CrowdStrike, Inc. All rights reserved.

CrowdStrike University

LOG 201: Preparing, Ingesting, and Parsing Log Data using Falcon LogScale

MODULE 1: DATA SOURCE PREPARATION

- Prepare and interact with log data within Falcon LogScale.
- Apply data mining techniques.
- Execute the data ingestion process.
- Recognize common challenges in log analysis and how to tackle them.
- Use normalization and optimization techniques to ready log data for analysis.
- Investigate various field types in Falcon LogScale.
- Utilize date and time formatting functions.

MODULE 2: INGEST, PARSE, EXPLORE AND SUMMARIZE DATA

- Implement data normalization, filtration and optimization techniques to eliminate false positives.
- Hunt for outliers and design strategies to reduce variance in your data sets.
- Develop strategies for enriching your data sets.
- Create and modify fields to enhance data analysis efficiency and accuracy at search time.
- Parse, extract, and normalize timestamps.

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

© 2023 CrowdStrike, Inc. All rights reserved.