EDU-2210
Using Search

Overview

In this one-day instructor-led course, students will learn the skills and features needed to effectively search the log data in the Exabeam Security Operations Platform. Log data is crucial for incident investigations. Learning to navigate and search through logs can help users reconstruct events, understand the scope of incidents, and gather evidence for further analysis. In this course, students will further their knowledge using hands-on labs and real-world exercises. They will learn how to use Search to filter for events, increase the power of searches using regex, and customize searches with advanced built-in tools such as Field templates and Field summary. By learning how to effectively search, students can build queries to identify patterns, anomalies, and potential security incidents, enabling quicker response times.

Objectives

Students will gain practical, hands-on experience with the features and functionalities of Search, Dashboards, and Correlation Rules. They will be challenged to demonstrate their comprehension throughout the course with the help of a course assessment, in-class activities, and lab exercises.

At the end of this course, students will be able to:

- Understand the capabilities of Search and how it works to help gain greater visibility and security.
- Describe the main elements of the CIM.
- Perform a search, view and narrow the search results, and share the search.
- Execute complex searches using regex, grouping, and other search tricks.
- Access educational resources in the Exabeam Training Center and Exabeam Community for additional learning and professional development.

Details

Duration	Role	Modality	Level
One day	Analyst, Security Engineer	Instructor-led	Intermediate

Prerequisites

- **Required:** Complete Fundamentals of the Common Information Model (CIM) (eLearning)
- **Recommended:** A basic understanding of IT and security concepts and a general awareness of cyberthreats

Intended Audience: This course is designed for analysts and other users who need to perform searches in Exabeam Security Operations Platform, as well as admins or engineers who need to build custom dashboards and correlation rules. This course is included as part of the Analyst learning path and the Security Engineer learning path.

Training Credits 1

Outline

Module 1: Using Search - Using elements of the Common Information Model, students will learn about performing queries in Search, creating visualizations and dashboards, and building correlation rules.

Module 2: How Information is Stored for Search - This module goes through the journey of a log and lists logging considerations. Students will also be able to describe the role of each Collector and recall what parsing does and recall the five key characteristics of the CIM.

Module 3: Start Searching - Students will author searches by working with fields and operators in the query builder and advanced search; they will also learn how to use the filtering options and Field Summary.

Module 4: Search Tips and Tricks - This module provides the opportunity for students to apply search tips and techniques to explore and get to know their data by using grouping, context filtering, and aggregations in Search.