Search, Dashboards, and Correlation Rules (EDU-2201)

Overview

Know how to author effective searches, as well as create and build amazing rules and visualizations. In this two-day instructor-led course, students will learn the skills and features behind Search, Dashboards, and Correlation Rules in the Exabeam Security Operations Platform. Students 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. They will also learn how to create complex visualizations simply in custom Dashboards and build meaningful custom alerts with Correlation Rules. Students will apply this information and build their skills through both lectures and hands-on labs. Because students will gain more competency in using the Exabeam Security Operations Platform with Search, Dashboards, and Correlation Rules, they will have increased visibility and better security for their organizations, at a lower cost per byte than the traditional SIEM.

Details

- **Duration:** Two days, instructor-led
- **Level:** Intermediate
- **Prerequisites:** Basic understanding of IT and security concepts and a general awareness of cyberthreats is required. A specific background in security tools, threat hunting, malware analysis, networking, or system administration is especially helpful.
- **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.

Detailed Outline

Module 01: Introducing the Exabeam Security Operations Platform

1. Review and discuss the purpose of the course, and key features of the Exabeam Security Operations Platform
2. Become familiar with the key takeaways in this course:
   1. Recall the elements of the Common Information Model
   2. Perform queries in Search
   3. Create visualizations and Dashboards
   4. Build Correlation Rules
3. Perform the following:
   1. Access and navigate the Exabeam Training Center
   2. Access and navigate the Community resources

Module 02: Journey of a Log

1. Describe the journey of a log and list logging considerations
2. Describe the role of each Collector
3. Recall what parsing does, and recall the five key characteristics of the Common Information Model

Module 03: Start Searching Data Lake

1. Recall the function and purpose of the Search application
2. Perform the following:
   1. Author searches in query builder and advanced search
   2. View and manipulate search results
   3. Filter search results
3. Work with fields and operators

Module 04: Search Tips and Tricks

1. Use techniques to discover your data
2. Use grouping in Search
3. Use regex in Search
4. Apply useful Search tips in your environment

Module 05: Get to Know Dashboards

1. Describe the benefits of tiles and Dashboards and identify which pre-built Dashboards are available
2. Navigate the Dashboard feature
3. Create a Dashboard with a basic table in five steps and define the following key terms:
   1. Dimension
   2. Measure

Module 06: Create Dashboards

1. Recall which type of visualization works best for certain types of data, then create additional chart types as examples
2. Use the pivot function and Dashboard filter tool to gain new views of the data

Module 07: Introducing Correlation Rules

1. Identify why to use Correlation Rules, including:
   1. Strengths and weaknesses of Correlation Rules
   2. Integration with the Threat Intelligence Service
   3. Contrasting Correlation Rules with modeling anomalies
2. Recognize where Correlation Rules fit in the Exabeam architecture, including:
   1. The Unified Ingestion Pipeline
   2. The Common Information Model
   3. Licensing entitlements

Module 08: Fundamentals of Correlation Rules

1. Discover the Correlation Rule creation workflows
2. Recognize rule condition logic
3. Define rule outcomes, including:
   1. Generating an alert
   2. Creating a case
   3. Sending an email
4. Finalize a Correlation Rule
5. Create a Correlation Rule to trigger when password spraying activity is detected

Module 09: Defining Correlation Rule conditions and types

1. Define rule types that evaluate matching events, including:
   1. "Any" rules
   2. Flatline rules
   3. Frequency rules
2. Define rule types that evaluate field values in matching events, including:
   1. Cardinality rules
   2. Change rules
   3. Metric aggregation rules
3. Define rule types that evaluate field values in matching events against a list, including:
   1. Allow list rules
   2. Block list rules
4. Identify and examine correlation rule templates
5. Practice creating correlation rules

Module 10: Manage, monitor, and troubleshoot Correlation Rules

1. Explore the rules page
2. Recognize correlation rules roles and permissions
3. Validate rule triggers using Search
4. Troubleshoot correlation rules

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, you should be able to do the following:

- Recall the capabilities of Exabeam Search, Dashboards, and Correlation Rules, and how they work to help gain greater visibility and security
- Describe the core components of the Exabeam Security Operations Platform
- Recall the main elements of the Common Information Model
- Perform a search, view and narrow the search results, and share a search
- Execute complex searches using regex, grouping, and other search tricks
- Recall the components of Dashboards and how to create a table visualization
- Create a variety of custom visualizations for Dashboards, and use additional features such as pivots and filters
- Identify when and why to use Correlation Rules
- Recall the components of a Correlation Rule and how to build Correlation Rules
- Manage, monitor, and troubleshoot Correlation Rules
- Access educational resources in the Exabeam Training Center and Exabeam Community for additional learning and professional development

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →