exabeam

DATA SHEET

EXABEAM DATA LAKE AND INCIDENT RESPONDER FOR SECURITY ANALYSTS (EDU-2250)

OVERVIEW

In this three-day instructor-led course, students will learn how to use the features and functionalities of Exabeam Data Lake and Exabeam Incident Responder (with Case Manager) to help them solve current security challenges. First, students will learn how to use the Data Lake interface to search and filter for events, increase the power of searches using Lucene, and customize searches with advanced search strategies. They will also learn how to create and export visualizations, create and share dashboards leveraging those visualizations, as well as scheduling and exporting out-of-box, Data Lake pre-populated, and vendor provided reports. Students will apply this information and build their skills through specific use cases. After this, students will learn how to streamline their workflows and increase analyst productivity with the help of Incident Responder and Case Manager. Because students will gain more competency in Data Lake and Incident Responder, they will have increased visibility and better security for their organizations, at a lower cost per byte than the traditional SIEM.

DETAILS

- **Duration:** Three days, instructor-led
- **Level:** Intermediate
- **Prerequisites:** Basic understanding of IT and security concepts and a general awareness of cyber threats 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 cyber-security analysts who use (or will be using) Exabeam Data Lake and Exabeam Incident Responder and Case Manager.
- **Note:** This course is designed for analysts and operators, not administrators or engineers.

OUTLINE

- **Module 01:** How Exabeam Empowers Security Teams - A description of Exabeam Security Management Platform and a high-level look at how Data Lake and the platform compare to recent and current SIEM solutions

- **Module 02:** How Data Lake Works - Answers basic questions about Data Lake architecture and data flow
- **Module 03:** Start Searching Data Lake - A hands-on exploration of the Data Lake interface touching on key functionalities and a look at basic search techniques
- **Module 04:** Perform Advanced Searches in Data Lake - Explores use cases and addresses advanced search features such as lists, exporting search results, and customizing searches
- **Module 05:** Create Visualizations and Dashboards in Data Lake - Hands-on practice creating and manipulating visualizations and dashboards
- **Module 06:** Create Reports in Data Lake - Contains demonstrations and discussions on how to utilize reporting feature within Data Lake, including out-of-box, Data Lake pre-populated, and vendor provided reports
- **Module 07:** How Data Lake Health Monitoring and Role-Based Access Works – Describes the important relationship between admin and analyst and how to customize roles
- **Module 08:** How Correlation Rules Work in Data Lake – Addresses how Data Lake can be configured with correlation rules for alerting, monitoring, and compliance checking
- **Module 09:** Increase Productivity with Incident Responder and Case Manager – Provides an overview of Incident Responder and Case Manager
- **Module 10:** How Case Manager Works – Answers basic questions about Case Manager including key terms and concepts
- **Module 11:** How Incident Responder Works – Answers basic questions about Incident Responder including service integrations
- **Module 12:** Start Streamlining Workflows – Demonstrates Incident Responder Playbooks and Case Manager in-action, showing how it impacts investigation workflows

OBJECTIVES

Students will gain practical, hands-on experience with the features and functionalities of Data Lake and Incident Responder, including use cases that they can apply within their own security workflow. 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:

- Identify the role of Data Lake in the Exabeam Security Management Platform
- Describe the simplified architectures surrounding Data Lake, including data flow through Data Lake
- Perform basic to advanced searches using the Exabeam Data Lake user interface and functionalities, including filtering, saving, exporting, customizing, tuning, and optimizing.
- Create visualizations using the following functionalities: linking chart type to new/saved search, Visualization Builder, and setting time filters and refresh rate.
- Create dashboards using the following functionalities: linking dashboards and visualizations or searches, and widgets.
- Demonstrate the following features of reports: importing, searching, downloading, sending, exporting templates, and scheduling.
- Recall how Exabeam's Incident Responder and Case Manager work with Advanced Analytics to help streamline incident response for greater security.
- Understand and utilize Incident Responder playbooks for Case Manager for automating and orchestrating incident response.
- Access additional educational resources in Exabeam's learning management system and Community for more learning and professional development.