exabeam

DATA SHEET

EXABEAM DATA LAKE FOR SECURITY ANALYSTS (EDU-2200)

OVERVIEW

In this two-day instructor-led course, students will learn how to use the features and functionalities of Exabeam Data Lake to help them solve current SOC/Security Team challenges. 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 such as, threat hunting, regulatory related searches, MITRE and NIST 800-61 related searching, data exfiltration incident scoping, and analytic processes (MITRE ATT&CK) that leverage searching, visualizations, dashboards, and reports.

DETAILS

- **Duration:** Two 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 for log data collection, indexing, and visualization.
- **Note:** This course is designed for analysts and operators, not administrators or engineers.

OUTLINE

- **Module 01: Why Data Lake Makes Sense** – An overview of Data Lake focusing on how Data Lake can help enable security teams, as well as be leveraged to help solve current SOC/Security Team challenges. Also includes a high-level overview of the Exabeam Security Management Platform, featuring a look at how Data Lake and the platform compare to recent and current SIEM solutions

- **Module 02: Architecture –** A look at the network and system architecture surrounding Data Lake, including an overview of Exabeam's Common Information Model (ECIM) and the data flow through Data Lake
- **Module 03: Scenic Tour of Data Lake (Walkthrough of Interface and Functionality) –** A hands-on exploration of the Data Lake interface touching on key functionalities
- **Module 04: Getting Started with Search Demo** – The first Data Lake product demo, focusing on search features and functionality, including the tipping point of Notables from Advanced Analytics and the transition to Data Lake

  Search Basics – An introduction to search functionalities, including Lucene and the structure of basic queries. Will also cover basic filtering, saving searches, using the library functionality, and results relating to log viewing
- **Module 05: Intermediate and Advanced Searching –** Going beyond basic searches by isolating search results, deeper dives with Lucene, using lists, exporting search results, and customizing searches. Advanced search strategies, including REGEX for conditions and filtering, excluding results, creating queries that leverage threat and intel feeds, and search tuning and optimization
- **Module 06: Search Use Cases –** Exploring use cases focused on using Data Lake for the following: threat hunting, regulatory related searches, MITRE and NIST 800-61 related searching, and incident response/handling
- **Module 07: Correlation Rules and Alerting –** A Data Lake Correlation Engine overview that discusses rule types and out-of-box/Data Lake pre-populated/vendor provided rules. Also covers referencing lists within rules, assigning or changing correlation rule alert severity, and rule troubleshooting/optimizing/suppression
- **Module 08: Visualizations and Dashboards Demo –** The second Data Lake product demo, focusing on visualizations, dashboards, reports, and out-of-box content related searching, and incident response/handling

  Visualizations – A Different Perspective on Data Lake Data - Creating visualizations in Data Lake, including chart type selection, linking chart type to a new/saved search, Visualization Builder, setting time filters and refresh rate, and sharing and downloading visualizations

  Dashboards – Creating Data Lake dashboards, including linking dashboards and visualizations or searches, widgets, saving, sharing, and exporting dashboards
- **Module 09: Reports –** Using reports within Data Lake, including out-of-box, Data Lake pre-populated, and vendor provided reports. Also, content that is contained within reports, as well as scheduling, exporting, sending, and deleting reports
- **Module 10: Incident Analysis Use Cases –** Exploring use cases focused on using Data Lake for the following: data exfiltration incident scoping and/or threat hunting methodology and analytic processes (MITRE ATT&CK) that leverage searching, visualizations, dashboards, and reports
- **Module 11: ("Nice to Have" - time permitting): Light Admin & RBAC/Role Based Access Controls –** A topic that starts to bleed into the administration side of Data Lake, so it may be included if there is room within the timeframe of the class. Possible topics include creating, editing, and maintaining users and groups, data retention (hot, warm, cold), backup and restore overview, and Role Based Access Control (RBAC)

OBJECTIVES

Students will gain practical, hands-on experience with the features and functionalities of Exabeam Data Lake, 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, including how Data Lake can help solve current SOC/Security Team challenges.
- Describe the simplified network and system architectures surrounding Data Lake and Exabeam's Common Information Model (ECIM), 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.
- Build correlation rules that alert on known bad or non-compliant behaviors.
- 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.