exabeam

DATA SHEET

EXABEAM SECURITY MANAGEMENT PLATFORM FOR SECURITY ANALYSTS (EDU-2500)

OVERVIEW

In this five-day instructor-led course, students will learn how to increase the velocity of their investigative tasks and improve their SOC workflows with the help of Exabeam Security Management Platform (Exabeam SMP: Data Lake, Advanced Analytics, Incident Responder). Students will learn the basics of UEBA and how to leverage Smart Timelines, risk scoring, and other features in Advanced Analytics to accelerate their daily tasks. They will learn how to execute advanced searches and create reports and visualizations in Data Lake, and how to integrate the Exabeam Security Management Platform into their security operations by creating cases and implementing playbooks using the case management tools in Incident Responder. They will also gain practice investigating specific use cases including insider threats, credential theft, lateral movements, and data exfiltration. With a gained competency in Exabeam SMP, students will have increased visibility and provide better security for their organizations, at a lower cost per byte than the traditional SIEM.

DETAILS

- **Duration:** Five 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 for monitoring and threat investigations.
- **Note:** This course is designed for analysts and operators, not administrators or engineers.

OUTLINE

- **Day 1: Preparing to Investigate with Advanced Analytics –** An important conversation about the core components in Advanced Analytics including user stateful tracking and risk scores. Learn the basics of Advanced Analytics architecture and answer core questions about models and rules. Day 1 also addresses MITRE ATT&CK, watchlists, and Threat Hunter in Advanced Analytics.

- **Day 2: Investigating Threats in Advanced Analytics –** Learn specific investigation workflows for reducing risk from insider threats, data exfiltration, credential theft, and lateral movement.
- **Day 3: Searching Data Lake** - A basic-to-advanced look at creating searches in Data Lake using Lucene, REGEX, filters, threat feeds, and more. Discuss the architecture of Data Lake, and learn how to search for MITRE ATT&CK techniques in the organization within Data Lake.
- **Day 4: Creating Alerts, Visualizations, and Reports in Data Lake –** Create visualizations and reports, and learn other useful tricks like scheduling reports, creating dashboards, import and export, and more.
- **Day 5: Integrating Exabeam SMP into Your SOC –** Learn how to add automation and orchestration (SOAR) into the SOC effectively and how to track and manage cases with Exabeam Incident Responder. Build integrated playbooks that improve security processes and accelerate response through semi or fully programmatic actions. Day 5 also addresses operational recommendations.

OBJECTIVES

Students will gain practical experience with the features of Exabeam SMP (Advanced Analytics, Data Lake, Incident Responder) including practice investigating specific use cases that they can then translate into their own security workflows. They will learn how to leverage advanced search capabilities with visualizations and integrate automation to gain greater visibility and accelerate security response. They will also learn how Exabeam aligns with industry frameworks and 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:

- Recall how behavior analytics, risk scoring, Smart Timelines™, and other core components in Exabeam Advanced Analytics work to help gain greater visibility and security.
- Leverage watchlists and threat hunter for higher velocity investigations, including TTP based searches.
- Begin translating common investigation workflows into Exabeam Advanced Analytics, starting with these use cases:
  - Insider Threats
  - Data Exfiltration
  - Privileged Access and Credential Theft
  - Lateral Movement
- 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.

- Identify the role of Incident Responder in the Exabeam Security Management Platform, including the purposes behind the core components and architecture.
- Create and track incidents end-to-end using integrated case management features.
- Demonstrate how to integrate automated response with drag-and-drop design and create practical playbooks using logic and flow charts.
- Access additional educational resources in Exabeam's learning management system and Community for more learning and professional development.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.