exabeam

Data Sheet

Digital Learning

Onboarding Data for Advanced Analytics (on-prem)

EDU-3500

Overview

In this five-day virtual-instructor-led course, administrators will learn how to configure the analytics components and the investigation capabilities of the Exabeam Security Management Platform. The purpose of this course is to prepare administrators to configure Advanced Analytics and to understand the Advanced Analytics processing pipeline. Administrators will also gain a better understanding of the processing pipeline so that analysts can benefit quickly from machine-learning, thus identifying threats quickly and effectively. This means a deep-dive into the stages of the data flow and how to configure the key analytical components in Advanced Analytics, including rules, models and parsers. Students will be using both the UI Settings controls and CLI in their labs.

The Exabeam Security Management Platform delivers an end-to-end prescriptive workflow to help organizations operationalize and deliver on their desired security outcomes.

Here's a brief description of how it works: the Exabeam Security Management Platform is an on-premises solution made up of applications (e.g. Advanced Analytics). Exabeam Advanced Analytics collects and processes data from strategically selected data sources (this may include Exabeam Data Lake) and third-party log management systems. This data is then processed by Advanced Analytics, which applies behavioral analytics, context enrichment, and threat intelligence. The results are presented to analysts in easy-to-use summary pages and Smart Timelines™ which in turn empower the SOC to respond to cyberattacks more rapidly and efficiently, while keeping overhead low and deployment times to a minimum. Configuring the components of the Exabeam Security Management Platform is critical to maximizing the SOC's operational efficiency, security strength, and desired security outcomes.

Objectives

Learn how to configure the administrative settings in Exabeam Advanced Analytics. Administrators will gain a firm grasp on how to configure Advanced Analytics and understand the processing pipeline which includes rules, parsers, events, and models. With the help of learning assessments, in-class activities, and lab exercises, instructors will work with you to strengthen and guide you through the course. This class is primarily designed for customers with on-premises installations of Advanced Analytics. However, in this class you will also learn the benefits of Exabeam cloud delivered services, including low infrastructure overhead and zero product maintenance without the need to purchase additional hardware to get your SOC up and running.

Details

Duration

Five days

Level

Intermediate

Modality

Instructor-led

Prerequisites

A basic understanding of Linux CLI and SSH is required; a background in SIEM and security technologies is highly recommended. Successful completion of Exabeam EDU Analyst training (EDU-1100 or EDU-2500).

Intended Audience

Administrative professionals within an organization who will be administering Exabeam within their organization's environment. It is not recommended for security analysts.

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

- Describe the components of the Exabeam Security Management Platform and the processing pipeline.
- Configure Advanced Analytics to customize the display of information in the UI.
- Configure Advanced Analytics to enable threat detection, investigation, and response.
- Identify and configure required administrator settings and have a firm grasp on log sources and ingestion methods, custom configuration best practices, and parsers.
- Create and troubleshoot event builders and describe their purpose.
- Describe the types, structure, and purpose of models and how confidence is calculated.
- Recognize rule types, structure, and purpose.
- Recall the purpose and function of the Advanced Analytics architectural components and identify the files associated with customization.

Outline

Day 1 : Architecture, Configuration, & Ingestion

Manage and maintain Advanced Analytics clusters to support sustainable incident response and threat hunting.

Day 2: Pipeline Processing & Parsing

Configure and troubleshoot Advanced Analytics using both GUI and CLI tools.

Day 3: Events & Sessions

Create structures and content including parsers, enrichers, models, and rules.

Day 4: Models & Rules

Customize and tune content to make analysts more effective, including minimization of both false positives and false negatives.

Day 5: Tuning & UI Customization

Access additional educational resources in Exabeam's learning management system and Community for more learning and professional development.