exabeam

Data Sheet | Instructor-Led

Advanced Analytics for Administrators

EDU-3101

Overview

This course is designed for the team that implements and supports the technical needs of Exabeam security analysts. Security engineers and SOC administrators will learn to plan, configure, and troubleshoot Exabeam Advanced Analytics.

Hands-on labs offer attendees both an opportunity to practice new concepts and a safe sandbox environment with which to experiment.

This course includes administrative concepts and configuration around Event Selection, Advanced Analytics, Case Manager, and Incident Responder. Please attend our EDU-2170 course for analyst-focused topics such as analytics, investigations, and threat hunting as this course focuses on administrative concepts.

Objectives

Students will gain practical experience configuring and troubleshooting Advanced Analytics, including practice optimizing existing rules and crafting custom rules. They will also learn how to tune Advanced Analytics to maximize and differentiate actionable incidents. They will be challenged to demonstrate their comprehension throughout the course with the help of daily assessments, in-class activities, and lab exercises.

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

- Manage and maintain Advanced Analytics to support sustainable incident response and threat hunting
- Configure Event Selection for log collection from both on-prem and cloud sources
- Create and customize rules
- Customize and tune content to make analysts more effective, including minimization of both false positives and false negatives
- Configure and customize Case Manager settings
- Access additional educational resources in Exabeam's learning management system and Community for more learning and professional development

Details

Duration
One day

Level
Intermediate

Modality
Instructor-led

Prerequisites
- **Required:** Complete the EDU-1402 (eLearning) Common Information Model (CIM).
- **Required:** Onboarding Data into the Exabeam Security Operations Platform (EDU-3201).
- **Recommended:** EDU-2170 Exabeam TDIR for Security Analysts before attending this course.

Intended Audience
This course is designed for administrators and engineers who will be configuring and maintaining Exabeam Advanced Analytics.

Outline

Subject to change

Module 1
Overview

Module 2
The Role of Collectors and Configuring Event Selection

Module 3
Advanced Analytics Architecture

Module 4
Advanced Analytics Initial Configuration

Module 5
Context and Event Enrichment

Module 6
Models and Data Insights

Module 7
Understanding and Creating Rules

Module 8
Case Manager Administration