EDU-4000

Deploying Exabeam Security Log Management and Exabeam SIEM

Overview

This five-day course is designed for engineers that deploy and configure Exabeam Security Log Management or Exabeam SIEM products for customers. Exclusively for Exabeam partners, this course is not available to customers.

The Exabeam deployment process is examined from start to finish and reinforced with hands-on labs. Configuration, log onboarding, and validation are highlighted. Engineers will also learn to minimize time to value by understanding how Exabeam products are used by security analysts.

Objectives

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

- Access and navigate the Exabeam Training Center, Community, and related documentation
- Understand the main architectural components of the Exabeam Security Operations Platform
- Describe the Common Information Model fields and hierarchical components
- Perform simple and advanced search activities, including narrowing, grouping, and regex
- Create a variety of custom dashboard visualizations that include pivot and filter functionality
- Identify correlation rule types and uses
- Create, manage, monitor, and troubleshoot correlation rules
- Configure and troubleshoot cloud-native and legacy Collectors including Site, Cloud, and Context Collectors
- Create, edit, and troubleshoot parsers using Log Stream
- Manage a successful Exabeam deployment

Details

Duration	Modality	Level
Five days	Instructor-led	Expert

Prerequisites

Basic understanding of Linux, APIs, and IT administration is required. Knowledge of IT administrative principles such as scripting is helpful but not required.

Intended Audience

Security engineers who will be deploying Exabeam products for customers.

Note

This course is composed of three separate courses: EDU-2201, EDU-3201, and EDU-4001. While consecutive attendance is recommended, the three courses may be taken individually.

Outline

Day 1

Introduction, Search, and Dashboards

Day 2

Correlation Rules creation and management

Day 3

Collectors — Site and Cloud — installation and configuration

Day 4

Collectors — Cloud and Context — configuration, parser creation and troubleshooting

Day 5

Exabeam SIEM benefits, Outcomes Navigator, APIs, and the Deployment Workbook

Detailed Outline

EDU-2201

Module 1

Introducing the Exabeam Security Operations Platform

- Become familiar with the purpose of this course and the Exabeam Security Operations Platform
- Access and navigate the Exabeam Training Center, Community, and Documentation portal

Module 2

Journey of a Log

- Describe the journey of a log and list logging considerations
- Describe the role of each Collector

Module 3

Start Searching

- Perform a search, narrow results, and share the search
- Work with fields and operators

Module 4

Search Tips and Tricks

- Discover the structures and values of your own data
- Use grouping and regex in Search

Module 5

Get to Know Dashboards

- Describe the benefits of dashboards and identify pre-built Dashboards
- Create a basic Dashboard using dimensions and measures

Module 6

Create Dashboards

- Understand and apply visualization types
- Use the pivot function and dashboard filter tool

Module 7

Introducing Correlation Rules

- Identify Correlation Rule types and uses
- Recognize where Correlation Rules fit in the Exabeam architecture

Module 8

Fundamentals of Correlation Rules

- Define Correlation Rule workflow and logic
- Create a Correlation ule to trigger when password spraying activity is detected

Module 9

Defining Correlation Rule Conditions and Types

- Define rule types that evaluate matching events and fields
- Examine correlation rule templates

Module 10

Manage, Monitor, and Troubleshoot Correlation Rules

- Recognize correlation rules roles and permissions
- Validate and troubleshoot rule triggers

EDU-3201

Module 1

Introducing Exabeam Log Onboarding

- Access training and education resources
- Recall the log ingestion process and Common Information Model

Module 2

Onboarding On-site Logs

- SaaS Site Collector concepts
- SaaS Site Collector core installation
- On-premises Site Collector concepts
- On-premises Site Collector installation and configuration
- New Collectors installation – Site

Module 3

Onboarding Cloud Logs

- Collector - Cloud concepts
- Configure Collectors - Cloud
- On-premises and SaaS Cloud Connector concepts
- Configure on-premises and SaaS Cloud Connectors

Module 4

Collecting Context Data

- Identify Context data in Exabeam Security Operations Platform
- Describe how the Collectors - Context and service works
- Configure a Context source
- Configure SaaS or on-premises context tables for Data Lake, Exabeam SIEM, or Exabeam Security Log Management

Module 5

Managing Ingestion with Log Stream

- Overview of ingestion
- Monitor and manage ingestion with Log Stream
- Manage and validate parsers in Log Stream and Live Tail

EDU-4001

Module 1

Greetings and Housekeeping

- Understand key takeaways
- Review systems used

Module 2

Features and Benefits

- Describe the high-level architecture of Exabeam Security Log Management and Exabeam SIEM
- Introduce Outcomes Navigator to demonstrate the closed-loop connection between log sources, parsing tiers, and outcomes

Module 3

Platform Overview

- Recall Exabeam Security Operations Platform features and components
- Use Outcomes Navigator to prioritize log sources and parsing effectiveness based on key customer scenarios

Module 4

Alert and Case Management

- Understand the purpose and roadmap of Alert and Case Management
- Recall event and incident creation methods and manage cases

Module 5

Using the Deployment Workbook

- Access and understand the deployment workbook
- Perform and track a deployment using Exabeam methodology

Module 6

Introducing Correlation Rules

- Create and manage API tokens
- Understand and use available API endpoints