Overview

In this five-day virtual-instructor-led course, you will learn how to increase the velocity of investigative tasks and improve security workflows with the help of Exabeam Fusion SIEM and the Exabeam Security Operations (SecOps) Platform. Learn the basics of Fusion SIEM and how to leverage Exabeam to accelerate daily tasks. Gain practice performing triage, investigation, detection, threat hunting, and incident response. You will also learn how to streamline workflows and increase analyst productivity with the help of Exabeam Case Management and Exabeam Threat Detection, Investigation, and Response Use Case Packages. Find out how to execute advanced searches and create reports and visualizations in Exabeam Data Lake. With an in-depth understanding of Fusion SIEM, you can have increased visibility, improved operational efficiency, and greater awareness of security outcomes for your organization.

Objectives

Gain practical experience with Fusion SIEM by practicing investigating specific use cases that you can translate into your own security workflows. Learn how Fusion SIEM aligns with industry frameworks. Find out how to achieve security outcomes with Exabeam TDIR Use Case packages. You will also gain practical experience with log management creating searches. With the help of a course assessment, in-class activities, and lab exercises instructors will work with you to strengthen and guide you during the course.
At the end of this course, students will be able to:

- Recall how the components of Fusion XDR work to help gain greater visibility and security; this includes XDR, UEBA, risk scoring, and Smart Timelines™.
- Leverage the incident lists, watchlists and Threat Hunter for higher velocity investigations, including TTP based searches
- Create and track incidents end-to-end using integrated case management features
- Describe how to achieve security outcomes using Exabeam Threat Detection Investigation and Response Use Case Packages
- Begin translating common investigation workflows into Advanced Analytics, starting with two of the three Exabeam use cases:
  - Compromised Insiders
  - Malicious Insiders
  - External Threats
- Recall how Exabeam Case Manager, Exabeam Incident Responder, and Exabeam Entity Analytics work with Advanced Analytics to help streamline incident response for greater security
- Identify the role of log management within the security operations platform, including how log management can help solve current SOC/Security Team challenges
- Perform basic to advanced searches using functionalities, including filtering, saving, exporting, customizing, tuning, and optimizing
- Create dashboards, visualizations, and reports
- Access to additional educational resources in Exabeam’s Training Center and Exabeam Community for more learning and professional development
Fusion SIEM Core Training for Security Analysts (EDU-2560)

Details

**Duration**
Five days

**Level**
Intermediate

**Note**
This course is designed for analysts and operators, not administrators or engineers.

**Modality**
Instructor-led

**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 Fusion SIEM. Maximum 12 attendees.

**Outline**

**Day 1: How Fusion SIEM works**
Answers basic questions about Fusion XDR including architecture, models, and rules. Also answers basic questions about user analytics and the Exabeam SecOps Platform including a close look into the Advanced Analytics interface.

**Day 2: Detect, Investigate, and Respond**
Includes how to use the incident lists, Notable Users, Notable Assets, watchlists, and threat hunting.

**Day 3: Use Cases**
Learn how Exabeam provides security outcomes through Exabeam TDIR Use Case packages. You will have access to two of the three Exabeam use case packages: Compromised Insiders, Malicious Insiders, and External Threats.

**Day 4: Search in Data Lake**
A basic-to-advanced look at creating searches in Data Lake using Lucene, REGEX, filters, threat feeds, and more. Includes topics that discuss the architecture of Data Lake.

**Day 5: 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.