Overview

In this three-day instructor-led course, you will learn how to increase the velocity of your investigative tasks and improve your security workflows with the help of Exabeam Fusion XDR and the Exabeam Security Operations (SecOps) Platform. Learn the basics of Fusion XDR core and how to leverage Smart TimelinesTM, risk scoring, and other features to accelerate daily tasks. You will gain practice investigating specific use cases such as compromised insiders, malicious insiders, and external threats. Find out how to streamline workflows and increase analyst productivity with the help of response automation. By learning the foundational concepts of behavior analytics, you will have increased visibility into your environment and provide better security for your organization.
Objectives

Gain practical experience with the behavior analytics features of Fusion XDR, including practice investigating specific use cases you can translate into your own security workflows. Learn how Fusion XDR aligns with industry frameworks. Knowledge checks are included to reinforce understanding as well as additional resources to ensure successful outcomes.

At the end of this course, you 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 Exabeam Fusion XDR, starting with two of the three available use cases:
  - Compromised Insiders
  - Malicious Insiders
  - External Threats
- Recall how case management, response automation and behavior analytics streamline incident response for greater security.
- Access to additional educational resources in Exabeam’s Training Center and Exabeam Community for more learning and professional development
Fusion XDR Core Training for Security Analysts (EDU-2160)

Details

Duration
Three 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 XDR. Maximum 12 attendees.

Outline

Day 1: How Fusion XDR 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 in Case Manager, and Notable Users, Notable Assets, watchlists, and Threat Hunter in Advanced Analytics.

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.