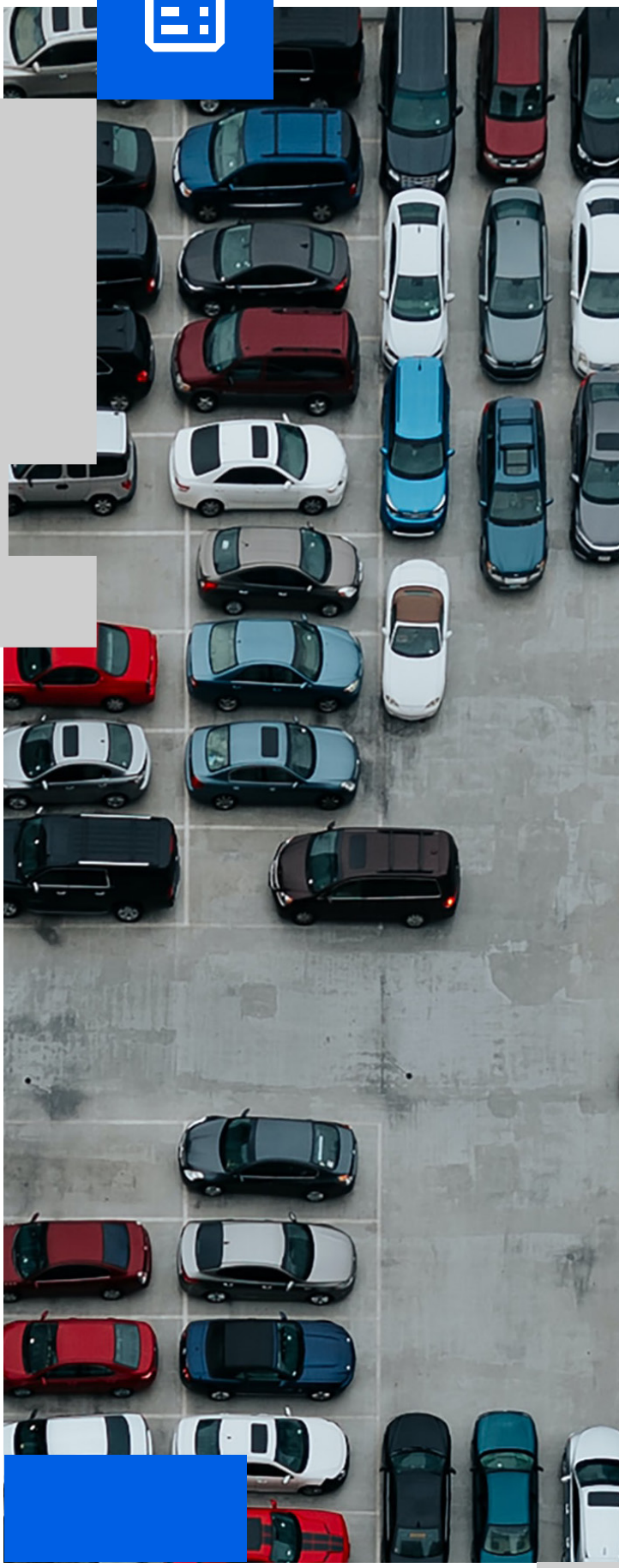
exabeam

Data Sheet | Digital Learning

Fusion XDR Training for Security Analysts

EDU-2170



Overview

In this three-day instructor-led course, you will learn how to increase the velocity of investigative tasks and improve 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. Throughout the course you will have opportunities to practice performing triage, investigation, detection, threat hunting, and incident response. Learn how to streamline workflows and increase productivity with the help of Exabeam Case Manager and Exabeam Threat Detection, Investigation, and Response Use Case Packages. Armed with knowledge about Fusion XDR, you will have increased visibility, improved operational efficiency, and greater awareness of security outcomes for your organization.

Objectives

Gain practical experience with the behavior analytics features of Fusion XDR, including practice investigating specific use cases that you can translate into your security workflows. Learn how Fusion XDR aligns with industry frameworks. Find out how you can achieve security outcomes with Exabeam TDIR Use Case packages. 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 Exabeam Fusion XDR, starting with these 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 Cener and Exabeam Community for more learning and professional development

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 incuding 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: Compromised Insiders, Malicious Insiders, and External Threats.