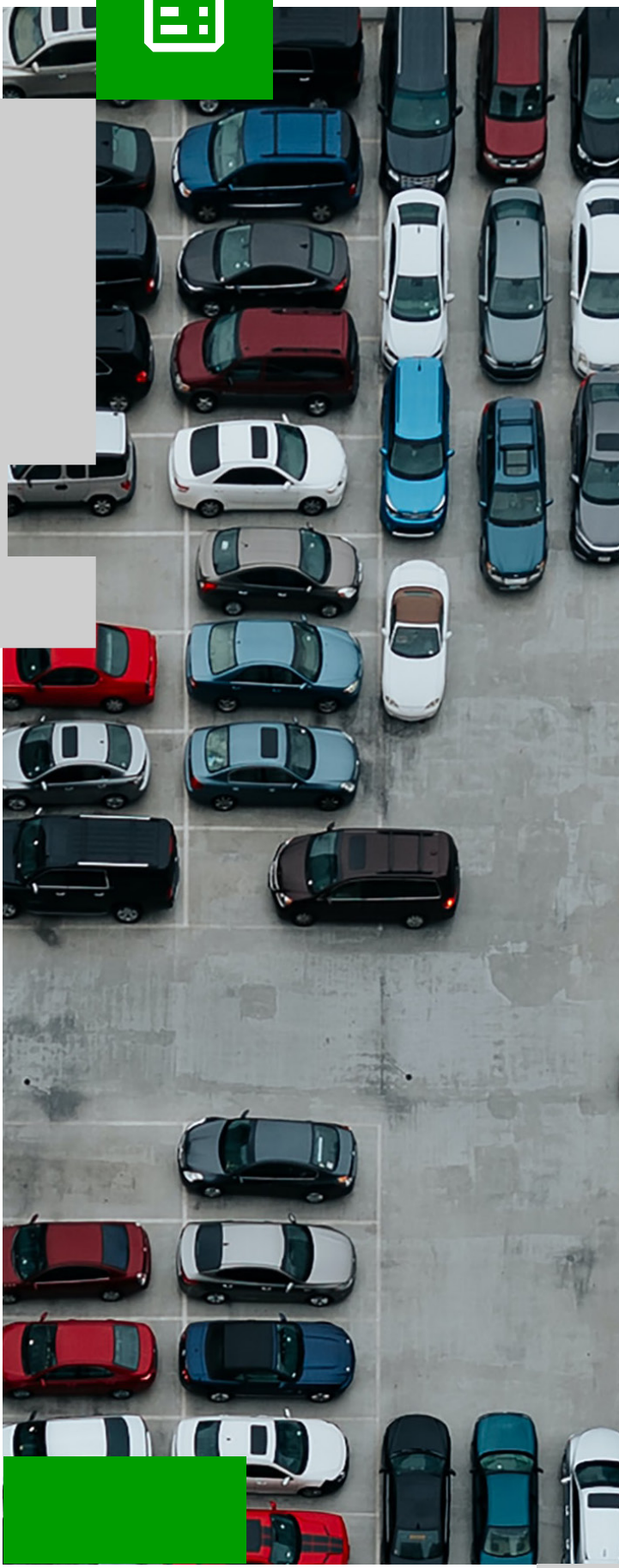
exabeam

Data Sheet | Instructor-Led

Exabeam TDIR Training for Security Analysts

EDU-2170



Overview

In this three-day virtual instructor-led course, students will learn how to increase the velocity of their investigative tasks and improve their security workflows with the help of Advanced Analytics and the Exabeam Security Operations Platform. Students will learn the basics of UEBA and how to leverage Smart Timelines™, risk scoring, and other features in Advanced Analytics to accelerate their daily tasks. They will gain practice performing triage, investigation, detection, threat hunting, and incident response. Students will also learn how to streamline their workflows and increase analyst productivity with the help of Case Manager and Threat Detection, Investigation, and Response Use Case Packages. Because students will gain more competency in Advanced Analytics, they will have increased visibility, improved operational efficiency, and greater awareness of security outcomes for their organization.

Objectives

Students will gain practical experience with Advanced Analytics. They will practice investigating specific use cases that they can then translate into their own security workflows. They will also learn how Advanced Analytics aligns with industry frameworks. They will learn how to achieve security outcomes with Exabeam TDIR Use Case packages. Students will be challenged to demonstrate their comprehension throughout the course with the help of a course assessment, in-class activities, and lab exercises.

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

- Recall how UEBA, risk scoring, Exabeam Smart Timelines™, and other core components in Exabeam Advanced Analytics work to help gain greater visibility and security
- 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 Exabeam Case Manager 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 these Exabeam use cases:
  - Compromised Insiders
  - Malicious Insiders
  - External Threats (malware, phishing, etc.)
- Recall how Exabeam Case Manager, Exabeam Incident Responder, and Exabeam Entity Analytics work with Advanced Analytics to help streamline incident response for greater security
- Access additional educational resources in the Exabeam Training Center 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
- **Required**: Complete the EDU-1402 (eLearning) Common Information Model (CIM).
- **Recommended**: 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) Advanced Analytics.

Outline

Day 1
How Advanced Analytics Works

Answers basic questions about Advanced Analytics architecture including models and rules. Answers basic questions about UEBA and close look into the interface.

Day 2
Detect, Investigate, and Respond

An important conversation about the analyst's workflow. 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 common use cases: Compromised Insiders, Malicious Insiders, and External Threats.