

EXABEAM ADVANCED ANALYTICS FOR SECURITY ANALYSTS (EDU-2100)

OVERVIEW

In this two-day instructor-led course, students will learn how to increase the velocity of their investigative tasks and improve their SOC workflows with the help of Exabeam Advanced Analytics and the Exabeam Security Management 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 also gain practice investigating specific use cases such as insider threats, credential theft, lateral movements, and data exfiltration. Because students will gain more competency in Advanced Analytics, they will have increased visibility and better security for their organizations, at a lower cost per byte than the traditional SIEM.

DETAILS

- **Duration:** Two days, instructor-led
- **Level:** Intermediate
- **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 Advanced Analytics.
- **Note:** This course is designed for analysts and operators, not administrators or engineers.

OUTLINE

- **Module 01: How Exabeam Empowers Security Teams** – A description of the Exabeam Security Management Platform with examples, and a look at education resources for further learning
- **Module 02: Get to Know Advanced Analytics** – An overview of Advanced Analytics including UEBA, the interface, and use cases
- **Module 03: How Advanced Analytics Works** – Answers basic questions about Advanced Analytics architecture including data flow, log sources, models and rules, and the deployment modes
- **Module 04: Prepare to Investigate Threats Using Notables, Watchlists, and Threat Hunter** – Addresses Notable Users, Notable Assets, watchlists, and Threat Hunter in Advanced Analytics

- **Module 05: Prepare to Investigate Threats Using Cybersecurity Frameworks** – An important conversation about frameworks including MITRE ATT&CK and a close look into the Advanced Analytics interface
- **Module 06: Start Investigating Insider Threats** – Discusses how to reduce the risk of insider threats, how to detect them in Advanced Analytics with lab practice
- **Module 07: Start Investigating Privilege Escalation and Credential Access** – Specific investigation workflow for reducing risk from privilege escalation
- **Module 08: Start Investigating Lateral Movement** – Specific investigation workflow for reducing risk from lateral movement
- **Module 09: Start Investigating Data Exfiltration** – Specific investigation workflow for reducing risk from data exfiltration
- **Module 10: Integrate Advanced Analytics into Your SOC** – Addresses operational recommendations and also summarizes the course content
- **Bonus Module: Ransomware** – A look at how Advanced Analytics detects ransomware.

OBJECTIVES

Students will gain practical experience with the UEBA features of Advanced Analytics, including 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 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 Exabeam’s UEBA, Risk Scoring, Smart Timelines, and other core components in Advanced Analytics work to help gain greater visibility and security
- Leverage Watchlists and Threat Hunter for higher velocity investigations, including MITRE ATT&CK TTP based searches
- Begin translating common investigation workflows into Exabeam Advanced Analytics, starting with these use cases:
 - Insider Threats
 - Data Exfiltration
 - Privilege Access and Credential Theft
 - Lateral Movement
- Access additional educational resources in Exabeam’s learning management system and Community for more learning and professional development

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT [EXABEAM.COM](https://www.exabeam.com) TODAY.