

EDU-3102

Rule Tuning for Advanced Analytics

Overview

Advanced Analytics has more than 1,500 built-in rules for threat detection. By gaining greater understanding in how rules work and how to edit the rule logic, students will be able to optimize their list of notables, amplify specific threats of interest, reduce the number of anomalies for a group of users or assets, and anticipate other useful rule tuning outcomes. When students are finished with this course, they will have the skills and knowledge needed to tune Advanced Analytics rules for greater accuracy, higher fidelity, and reduced noise. Students will also improve their security workflows with optimized Advanced Analytics rules. The course begins by outlining why rule tuning is necessary and useful. It then gives students practical knowledge of how rules work, describing the anatomy of a rule in detail. This is followed by the functions and operators available in rule expressions, and how to edit them. Finally, the course guides students through a rule tuning methodology, from assessing their current rules to recommendations and best practices for “tuning down” or “tuning up,” as well as other important considerations.

Objectives

This course's purpose is to develop a strong understanding of why rule tuning is necessary, and enable learners to create and edit Advanced Analytics rules for optimization. Students will gain practical experience with Advanced Analytics rules and tuning those rules. They will be able to describe why rule tuning is necessary and when to tune rules. They will be able to describe the anatomy of an Advanced Analytics rule and become familiar with the different field attributes. Students will use this knowledge to edit rule expressions using a variety of functions, while following best practices and a methodology for rule tuning. 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:

- List reasons why rule tuning is necessary and useful
- View a rule in Advanced Analytics and describe the two types
- Describe how risk scores are calculated
- Recall the different types of context in Advanced Analytics and create a context table for use with a rule
- Describe the attributes of a rule and its dependencies
- Summarize what is meant by “rule tuning” and make basic rule adjustments
- Edit rule logic and use available rule functions
- Utilize “include” and “exclude” logic to improve rule fidelity
- Utilize variable scoring in rules to improve rule fidelity
- Follow a methodology to “tune down” noisy rules
- Follow a methodology to “tune up” rules for business or security reasons
- Use tips and tricks for rule tuning including:
 - Updating context tables
 - Visualizing the anomalies
 - Creating a rule tuning tracker
- Access additional educational resources in the Exabeam Training Center and Exabeam Community for more learning and professional development

Details

Duration	Modality	Level	Role
One day	Instructor-led	Intermediate	Security Engineer

Prerequisites

- Required:** Advanced Analytics Administration (EDU-3101) and TDIR for Security Analysts (EDU-2170); prior working knowledge of Advanced Analytics technology.
- Recommended:** Supporting eLearning modules.

Intended Audience

Security engineers or individuals responsible for operationalizing and optimizing the threat detection features of Advanced Analytics.

Related Products

Exabeam Fusion, Exabeam Security Investigation, Exabeam Security Analytics

Outline

Module 1: Why Tune Rules in Advanced Analytics?

Course overview and introduction; answer basic questions such as: "What is rule tuning?" and "Why tune rules?"

Module 2: Recommendations for Rule Tuning

Follow a methodology and learn best practices.

Module 3: How Advanced Analytics Rules Work

Rule types, fields, and attributes; learn about rule dependencies and the role of context tables with rules.

Module 4: Editing Rule Logic

Dig into editing the rule expression and using functions; learn several techniques such as include/exclude and variable rule scoring.