FORCEPOINT

Forcepoint Behavioral Analytics (FBA) Fundamentals – Virtual Instructor-led

Datasheet

March 2019

Forcepoint Behavioral Analytics (FBA) Fundamentals

FBAFUND

Course Overview

In this virtual instructor-led training course, you learn how to navigate the Forcepoint Behavorial Analytics user interface, determine Information Security (INFOSEC) and Regulatory Surveillance use cases, and examine the FBA analytic building blocks. You also learn how to perform Basic and Advanced searches and write search queries using the Query Language (RQL).

Audience

Personas include: Reviewers, Analysts, Investigators, Data Engineers, Administrators, Technical Support, Sales Engineers

Course Objectives

- Define how Forcepoint Behavioral Analytics (FBA) focuses on insider risk.
- Distinguish FBA from similar products.
- Navigate the FBA environment including the Review and Analytic dashboards.
- Describe the interactions between the FBA architectures' primary components.
- Identify and define how entities and events relate to FBA.
- Examine the analytic blocks: Features, Models, and Scenarios.
- Examine how Features, Models, and Scenarios define individual risk scores.
- Use Basic and Advanced search to find entities and events and examine the results.
- Examine the use cases that FBA supports, such as INFOSEC and Regulatory Surveillance, and how those use cases can be applied in your FBA environment.
- Determine how to use the analytics building blocks to locate bad actors in your environment.
- Refine your search capabilities by using basic search, writing and saving advanced searches using RQL.

Prerequisites for Attendance

- You must have a working knowledge of advanced computer terminology, including networking, security, and Internet terms.

Format:

Virtual Instructor Led Training*

Duration:

8 hours total - 2 sessions, 4 hours per session. In addition, you can expect 1-2 hours of homework per session, plus 2 hours for the certification exam.

Language:

English

Course Price:

$700 USD

Exam Price:

Included

Certification Exam Information

This course prepares you for the FBA Fundamentals certification exam. The exam is included in the course price and is taken online after completion of the course at your leisure within 6 months of completion. You must score a minimum of eighty-percent (80%) to obtain certification. There is no performance-based exam.

Course Outline

Module 1: Introducing Forcepoint Behavioral Analytics (FBA)

- Identify various types of IT security risks utilizing FBA.
- Define how insider risk is addressed by FBA.
- Describe key FBA capabilities.
- Explain how user data is addressed by privacy protection regulations, such as General Data Protection Regulation (GDPR).
- Compare Regulatory Surveillance and INFOSEC use cases.
- Describe the interactions between the FBA architectures' primary components.
- Describe Modes, Events and Entities.
- Identify the FBA analytic building blocks: Features, Models, and Scenarios.
- Explain how FBA fits into the Forcepoint Human Centric System.
- Explain the Risk Adaptive Protection concept.

Module 2: FBA Events and Entities

- Examine FBA Events to define its Mode, Attributes, Entity roles, and Features.
- Review Events by adding Notes, Labels, and Review statuses.
- Describe various kinds of Entities depending on their roles.
- Define Monitored Entities, resolved name versus raw names, aliases, risk levels, and scores.
- Use the Basic search form to search by filtering.
- Explain the search results from various aggregate reports.

Module 3: Filtering Events and Saving Searches

- Use on-line documentation to write short RQL queries.
- Restore omitted field names and follow guidelines to make RQL queries readable.
- Convert between Basic and Advanced search.
- Filter Events by label and review status.
- Explain saved searches and how they populate the Review Dashboard.

Additional Information

**To attend this virtual online course, you must have a computer with:*
- *A high-speed internet connection (minimum of 1MB connection required)*
- *An up to date web browser (Google Chrome recommended)*
- *Adobe Flash web browser plug in (v13 or higher)*
- *PDF Viewer*
- *Speakers and microphone or headset (headset recommended)*

A separate tablet or ebook reader is also recommended for the course and lab book delivery

Terms and Conditions

- Virtual Instructor Led Trainings (VILT's) are delivered as live instructor-led training in an online classroom - No onsite delivery element.
- This course is limited to the topics described in this data sheet and may not address all of your unique requirements.
- Forcepoint training courses are standard and non-negotiable.
- Forcepoint provides the training "AS IS" and makes no warranties of any kind, express or implied.
- VILT's courses must be completed within 6 months from purchase or the course may be forfeited.
- The training services in this course are provided pursuant to the Subscription Agreement.
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions.

For more information about this course or other Forcepoint training offerings, please visit:
https://www.forcepoint.com/services/training-and-technical-certification
or contact Forcepoint Technical Learning Services at learn@forcepoint.com