Forcepoint Insider Threat Administrator Virtual Instructor-led

Datasheet

August 2019

Forcepoint Insider Threat Administrator Virtual Instructor-led

SVITADM

This Virtual Instructor-Led Training (VILT) course provides in-depth instruction for teams starting out with a Forcepoint Insider Threat deployment and those who need to learn to operate the system independently. This course includes operator management, agent creation and deployment, basic policy construction, basic investigations, system administration, and reports. There is substantial hands-on interaction, enabling the analyst to discern malicious from benign user activity.

Audience

- Consultants, System Architects, Integrators and Planners who help customers with Forcepoint Insider Threat implementations
- System Administrators, Network Security Administrators, IT staff and Forcepoint Insider Threat Operators

Course Objectives

- Articulate the fundamentals of the Insider Threat
- Apply best practices for configuration and implementation
- Describe and utilize controls and capabilities in all Forcepoint Insider Threat Workbenches
- Investigate and respond to potential threats
- Create and install the Forcepoint Insider Threat Agent
- Operate and configure the Investigation Workbench
- Create policies in the Policy Workbench
- Test and customize Forcepoint Insider Threat policies
- Utilize the Administration Workbench tools to create and map groups
- Manipulate the Command Center to analyze threat / risk of users
- Provide reporting on user and system behavior
- Understand essential system administration functions

Format:
Virtual Instructor-led*

Duration:
16 hours total - 4 sessions, 4 hours per session – plus 30-60 minutes of homework each session

Language:
English

Course Price:
$1,150 USD non-discountable

Exam Price:
Included

Prerequisites for attendance

- General understanding of system administration and Internet services.
- Basic knowledge of networking and computer security concepts.
- A computer that meets the requirements noted at the end of this document.

Certification Exam

This course prepares you to take and pass the Certified Forcepoint Insider Threat Administrator Exam. The exam is included in the price of the course but the execution of the exam is not accomplished during the course. A minimum score of 80% on the multiple choice online exam is required to obtain certification.

"It was a great course that really helps understanding the overall administration of Insider Threat."

Course Outline

MODULE 1: THE INSIDER THREAT PROBLEM

- Describe the high-level overview of components and their primary function
- Review and setup virtual lab environment
- Identify the updates and features added to FIT in version 8.1 to 8.1.4
- Understand the critical pieces that make up working FIT deployments and how to access the system
- Manage operator accounts and roles in Command Center

MODULE 2: SYSTEM OVERVIEW

- Comprehend the Enterprise Application Suite capabilities and workflow
- Understand and compare risk scores in FIT
- Investigate users starting in Command Center and continuing with Enterprise Application Suite (EAS)
- Perform administration and policy configuration in EAS
- Articulate the Command Center Workflow
- Create agent installer from the Administration Workbench
- Deploy agents and assign them to groups
- Analyze user behavior to know how it affects their risk score to be able to fine tune policies and access true risk

MODULE 3: EAS WORKBENCHES

- Use Investigation Workbench to identify Risky Users, Create Cases, and Run Reports
- Create and Customize Policies in Policy Workbench
- Manage Agents and Users with Administration Workbench
- Analyze Agents by a variety of parameters to determine if there are performance or configuration issues
- Create policies and investigate resulting events and collections
- Utilize the Administration Workbench to analyze users and agents in detail
- Manage Group membership for operator access security

MODULE 4: MAINTENANCE AND INTEGRATIONS

- Understand settings available in Command Center
- Articulate which features rely on integration
- Configure and test the DLP/FIT integration
- Navigate the appliance admin console
- Understand the various integrations with products external to FIT
- Comprehend and monitor the Command Center dashboards
- Run final lab on: Deploy agents, Create and test policies, Investigate risky behavior

**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 e-book 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