Forcepoint Insider Threat System Engineer Instructor led
FITIMP

During this 5-day hands-on instructor led course, you will gain an understanding of the key core competencies and skills needed to practice as a System Engineer handling Forcepoint Insider Threat. The core competencies are design, deployment, integration, maintenance, and troubleshooting. This course prepares engineers or other professionals who are about to manage or lead system engineering development of Forcepoint Insider Threat from concept creation to production.

Audience
- Consultants, system architects, integrators and planners who help customers with Forcepoint Insider Threat implementations
- Sales Engineers, Implementation Specialists, Deployment Specialists, Network Architects, Technical Support

Course Objectives
- Understand key FIT deployment types.
- Learn about sizing and performance considerations.
- Understand how Insider Threat integrates with other Forcepoint products and third-party products.
- Perform common maintenance activities to keep system performance high in fast-evolving real-world environments.
- Troubleshoot and debug each major component.

Prerequisites for attendance
- Completion of the Forcepoint Insider Threat Administrator Course and certification.
- Intermediate knowledge of networking and computer security concepts.
- A computer that meets the requirements noted at the end of this document.

Format:
Instructor Led In-person*

Duration:
40 hours total - 5 days, 8 hours per day – plus 30-60 minutes of homework each session

Language:
English

Course Price:
$3,500 USD non discountable

Exam Price:
Included

Certification Exam
This course prepares you to take and pass the Certified Forcepoint Insider Threat System Engineer 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.
Course Outline

MODULE 1: COMPONENTS AND COMMUNICATION
- Describe the responsibilities of each component
- Understand protocols and ports used for communication between components

MODULE 2: PLANNING
- Identify and confirm key System Requirements
- Provide sizing guidelines based on number of agents and policy weight
- Accommodate for growth and redundancy specifications

MODULE 3: INSTALLATION
- Perform demos, Proof of Concepts (POCs), and simple deployments
- Complete intermediate appliance-based deployments
- Configure advanced clustered deployments for large enterprises

MODULE 4: INITIAL CONFIGURATION
- Complete global setup checklist
- Complete Administration Workbench agent setup checklist
- Complete Policy Workbench checklist

MODULE 5: PHASED ROLLOUT DEPLOYMENTS
- Implement best practices for initial rollout
- Configure and Install Windows Agent
- Configure and Install Mac OS X Agent

MODULE 6: TUNING
- Create, test, and tune advanced level policies to address a variety of customer’s insider threat concerns

MODULE 7: ADVANCED AGENT DEPLOYMENT
- Complete roll out using remote Agent deployment solutions

MODULE 8: BACKUP AND DISASTER RECOVERY
- Set up backups and confirm them with a test recovery

MODULE 9: MONITORING
- Track deployed Agents using Administration Workbench
- Run and review reports to preempt potential performance issues

MODULE 10: PERFORM AP-DATA INTEGRATION
- Test and tune AP-DATA triggered policies
MODULE 11: SET UP GROUP MAPPING VIA LDAP INTEGRATION
- Import Active Directory fields for additional context
- Configure group mapping to sync policies with LDAP group membership

MODULE 12: UNDERSTAND THE CAPABILITIES OF CONVERGENCE AND SPOTLIGHT APIS
- Convergence API for aggregation of external data into FIT
- Spotlight API for exporting behavioral data to additional analytics engines

MODULE 13: SERVER UPGRADES
- Prepare deployment and database for hotfix
- Install Hotfix
- Reinitialize database and test deployment

MODULE 14: AGENT BUNDLE UPGRADES AND COMPATIBILITY PACKS
- Upgrade using agent commands
- Upgrade using remote install utility

MODULE 15: VERIFICATION
- Confirm HF and Agent Bundles perform as expected

MODULE 16: TROUBLESHOOTING METHODOLOGY
- Correctly identify the root cause
- Apply and confirm a solution

MODULE 17: PERFORM CRITICAL SERVER DIAGNOSTICS
- Enable and review verbose logging
- Access appliance using debug account

MODULE 18: DATABASE DIAGNOSTICS AND MAINTENANCE
- Administer Oracle databases using sqlplus
- Manage database using Oracle Enterprise Manager (OEM)

MODULE 19: AGENT MONITORING AND TROUBLESHOOTING
- Run Agent Tool diagnostics locally and remotely
- Use Agent Tool to test for configuration issues
- Manage Agents remotely
- Enable and view verbose logging
Terms and conditions

Forcepoint products may be used to address customer concerns regarding content that could be considered objectionable or offensive. As a result, portions of Forcepoint course materials and lab exercises that train on these products may use examples of such content to teach appropriate protection mechanisms. Enrollees should be aware of this possibility, and if they are concerned should not enroll in this course or should consider purchasing a custom course that could be created to utilize other examples.

Additional terms and conditions found here:
https://www.forcepoint.com/resources/training/forcepoint-training-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