



Forcepoint Insider Threat

CERTIFIED SYSTEM ENGINEER INSTRUCTOR LED COURSE



Forcepoint Insider Threat System Engineer Course

COURSE OVERVIEW

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.

CERTIFICATION EXAMS

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.

Format:

Instructor Led In-person

Duration:

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

Price:

\$7,000 USD non-discountable

Language:

English

COURSE DAILY AGENDA

SESSION 1 DESIGN AND DEPLOYMENT

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

SESSION 2 DESIGN AND DEPLOYMENT CONTINUED

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



SESSION 3 INTEGRATIONS

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

SESSION 4 UPGRADES AND HOTFIXES

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

SESSION 5 TROUBLESHOOTING AND DEBUGGING

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

- System Engineer trainings are limited and may not address all of your unique requirements
- The training services in this course are provided pursuant to the Subscription Agreement
- Forcepoint provides the System Engineer course “AS IS” and makes no warranties of any kind, express or implied
- You must register for the System Engineer course offering within 90 days of the Order or the course is forfeited
- System Engineer courses must be completed within 6 months from purchase or the course is forfeited
- Assent to the Subscription Agreement constitutes acceptance of the above terms and conditions

For more information about other Forcepoint training offerings, please visit our [Customer](#) or [Partner](#) training page.

Questions about Forcepoint training? Contact Forcepoint Technical Readiness and Training at salestraining@forcepoint.com

