DEEP SECURITY TRAINING FOR CERTIFIED PROFESSIONALS

DURATION: 3 DAYS

COURSE OVERVIEW

In this course, you will learn how to use Trend Micro™ Deep Security. This course provides information about the basic architecture, deployment scenarios, installation processes, policy configuration and administration options, as well as troubleshooting details that a network administrator needs to know for successful implementation and long-term maintenance.

TARGET AUDIENCE

This course is designed for IT professionals who are responsible for protecting networks from any kind of networked, endpoint, or cloud security threats.

The individuals who will typically benefit the most include: System administrators / Network engineers / Support Engineers / Integration Engineers / Solution & Security Architects

COURSE CONTENT

Overview

1. Key Functionality
2. Components and Architecture
3. Installation Planning and Deployment
4. Product In-Depth
5. Deep Security Manager and Agent
6. Update and Software Management
7. Integration
8. Endpoint Management
9. Detection Methods and Agent Activation
10. Deep Security Relays
11. Security Updates
12. Policy Management

13. Inheritance, Hierarchy, and Overrides
14. Common Objects
15. Anti-Malware Solution Platform (AMSP)
16. Anti-Malware Scan Engines
17. Scans and Quarantine
18. Smart Protection
19. Web Reputation
20. Security Levels and Exceptions
21. Web Reputation Communication
22. Analysis Process
23. Firewall
24. Firewall Rules
25. Reconnaissance Scans
26. Traffic Analysis
27. Intrusion Prevention
28. Virtual Patching
29. Protocol Hygiene
30. Application Control
31. Web Application Protection
32. Recommendation Scans
33. Integrity Monitoring
34. Event Tagging
35. Log Inspection
36. Logging and Reports
37. Multi-Tenancy
38. Agentless Protection
39. Cloud Computing
40. Amazon AWS, Microsoft Azure and VMware v Cloud

COURSE PREREQUISITES

Before you take this course, Trend Micro recommends that you have a working knowledge of their products and services, as well as basic networking concepts and principles.

You should also have a working knowledge or understanding of the following:

1. Windows servers and clients
2. Firewalls, WAFs, Packet Inspection devices

3. Microsoft Internet Information Server (IIS), Apache
4. VMware ESXi / v Center / v Shield
5. Amazon AWS / Microsoft Azure / VMware v Cloud
6. Virtualization techniques and technologies