TRAPS 3.4: INSTALL, CONFIGURE, AND MANAGE (EDU-281)

Overview

Palo Alto Networks® Traps™ Advanced Endpoint Protection prevents sophisticated vulnerability exploits and unknown malware-driven attacks. Successful completion of this two-day, instructor-led course equips the student to install Traps in basic configurations.

SESSIONS

Mod 1: Traps Overview
- How sophisticated attacks work today
- The design approach of Traps
- Main features of Traps
- Traps resources

Mod 2: Installing Traps
- Planning the installation
- Installing ESM Server and database
- Installing ESM Console
- Installing agents
- Managing content updates
- Upgrading Traps

Mod 3: Malicious Software Overview
- Exploitation techniques and their prevention
- Malware techniques and their prevention

Mod 4: Consoles Overview
- Introduction to ESM Console
- Introduction to the Traps Agent Console

Mod 5: Traps Protection Against Exploits
- Architecture and overview
- Configuring exploit protection

Mod 6: Traps Protection Against Malware (including WildFire)
- Architecture and Overview
- WildFire
- Local Analysis
- Trusted Publishers
- Malware Restrictions and Malware Protection Modules

Mod 7: Managing Traps
- System monitoring
- License administration
- Important server and agent settings
- Agent actions

Mod 8: Traps Forensics
- Forensic information retrieval
- Responding to prevention events

Mod 9: Basic Traps Troubleshooting
- Troubleshooting Resources
- Working with Technical Support
- Troubleshooting scenarios

Course Objectives

Students will learn how Traps protects against exploits and malware-driven attacks. In hands-on lab exercises, students will install and configure the Endpoint Security Manager (ESM) and Traps endpoint components; build rules; enable and disable process protections; and integrate Traps with Palo Alto Networks WildFire™, which provides prevention and detection of zero-day malware.

Scope

- **Course level:** Introductory
- **Course duration:** 2 days
- **Course format:** Combines instructor-facilitated lecture with hands-on labs
- **Software version:** Palo Alto Networks Traps Advanced Endpoint Protection 3.4

Target Audience

Security Engineers, System Administrators, and Technical Support Engineers

Prerequisites

Students must have Windows system administration skills and familiarity with enterprise security concepts.

Training from a Palo Alto Networks Authorized Training Center delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications give you the Next-Generation Security Platform knowledge necessary to prevent successful cyberattacks and safely enable applications.

4401 Great America Parkway
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com