TRAPS 4.1: 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 helps prepare the student to install Traps in basic configurations.

Module 1: Traps Overview
- How sophisticated attacks work today
- The design approach of Traps
- Traps components
- Traps resources

Module 2: Installing Traps
- Planning the installation
- Installing ESM Server and Console
- Installing Windows agents
- Installing Mac Agents
- Managing content updates
- Upgrading Traps

Module 3: Malicious Software Overview
- Basics of computer architecture
- Exploitation techniques and their prevention
- Malware techniques and their prevention

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

Module 5: Traps Protection Against Exploits
- Architecture and EPMs
- Configuring exploit protection

Module 6: Traps Protection Against Malware (including WildFire)
- Malware protection process flow and components
- Post-detection malware anaylsis

Module 7: Managing Traps
- System monitoring
- Traps license administration
- Agent license administration
- Server settings, users, and roles
- Agent settings
- Agent actions

Module 8: Traps Forensics
- Forensics workflow and policies
- Responding to prevention events
- Logging

Module 9: Basic Traps Troubleshooting
- DIReC methodology
- Troubleshooting resources
- Working with technical support
- Troubleshooting installation, connectivity, and upgrades

Course Objectives

Students should 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 4.1

Target Audience

Endpoint Security Engineers, System Administrators, and Technical Support Engineers

Prerequisites

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

Palo Alto Networks® Education

Training from Palo Alto Networks and Palo Alto Networks® Authorized Training Centers delivers knowledge and expertise that prepare you to protect our digital way of life. Our trusted security certifications validate your knowledge of the Palo Alto Networks® next-generation security platform and your ability to help prevent successful cyberattacks and safely enable applications.

3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com