TRAPS: CLOUD SERVICE OPERATIONS (EDU-290)

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 configure the Traps Management Service and to install Traps onto endpoints.

Module 1: Traps Overview
- How Sophisticated Attacks Work Today
- Traps Multi-Method Threat Prevention
- Traps Components and Resources

Module 2: Cloud Services
- Application Framework and Cloud Services Portal
- Shared Services and Traps Onboarding Flow

Module 3: Cloud- Based Management
- Traps Service Dashboard and Licensing
- Cross-Platform Agent and Agent Installation
- Endpoints and Endpoint Groups

Module 4: Policy Rules and Profiles
- Profiles and Policy Rules
- Agent Settings Profile

Module 5: Malware Protection Flow
- Traps Malware Protection Modules Overview
- Restrictions Profiles, Malware Profiles, and Scanning

Module 6: Exploits and Exploitation Techniques
- Application Exploit Prevention
- Exploitation Techniques and Defense Mechanisms
- Basics of Process Management (Optional)

Module 7: Exploit Protection Modules
- Architecture and Overview
- Exploit Protection Modules (EPMs)
- Exploit Profiles

Module 8: Event Management
- Security Event Logs and Exceptions
- Endpoint and Server Logs
- Manage Quarantined Files

Module 9: Basic Traps Troubleshooting
- Troubleshooting Methodology and Resources
- Traps Cytool and Agent Identification
- Traps Agent Log Files and Agent Persist Databases
- Working with Technical Support

Module 10: Traps Architecture
- AWS Services Used by Traps Service
- Multi-Regional Architecture
- Agent File Uploads and Downloads
- Agent-Server Communication

Module 11: Directory Sync Service
- Directory Sync Service – Activation and Setup
- Troubleshooting

Course Objectives

Students should learn how Traps protects against exploits and malware-driven attacks. In hands-on lab exercises, students will explore and configure new cloud-based Traps Management Service and install Traps endpoint components; build policy rules and profiles; enable and disable process protections; and integrate Traps with Palo Alto Networks WildFire® cloud service, 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

Target Audience

Endpoint Security Engineers, System Administrators, and Technical Support Engineers

Prerequisites

Students must have 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® Security Operating 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