TRAPS 6.1: CLOUD SERVICE OPERATIONS (EDU-290)

Overview

Palo Alto Networks Traps Advanced Endpoint Protection prevents sophisticated zero-day exploits and unknown malware-driven attacks. Successful completion of this two-day, instructor-led course helps prepare the student to provision and configure the Traps management service and to install the Traps agent onto endpoints.

Module 1: Traps Overview
- Traps Multi-Method Threat Prevention
- Traps Components and Resources

Module 2: Working with Cortex Apps
- Cortex and the Hub
- Traps Onboarding Flow

Module 3: Traps Management Service
- Traps Management Service Web Interface
- Traps Agents and Agent Installations
- Endpoints and Endpoint Groups
- Policy Rules and Profiles

Module 4: Traps Malware Protection
- Traps Malware Protection Overview
- Restrictions Profiles and Malware Profiles
- Behavioral Threat Protection

Module 5: Traps Exploit Protection
- Application Exploit Prevention and Exploitation Techniques
- Exploit Protection Modules and Exploit Profiles
- Basics of Process Management (Optional)

Module 6: Managing Security Events
- Security Events
- Exceptions
- Response Capabilities
- Automatic Dump Analysis

Module 7: Traps Troubleshooting
- Troubleshooting Methodology and Resources
- Traps Cytool Application
- Server Logs, Agent Logs, and Agent Data Stores
- Working with Technical Support

Module 8: Agent-Server Communications
- Multi-Regional Architecture
- Agent-Server Communication

Module 9: Cortex Infrastructure Services
- Shared Services
- Log Forwarding App
- Directory Sync Service

Module 10: Advanced Operations
- The XDR Initiative
- Linux Container Protection
- Android Endpoint Protection (Optional)

Course Objectives

This course explains how Traps protects against exploits and malware-driven attacks. Hands-on lab exercises help students provision and then explore and configure the cloud-based Traps management service, install the Traps agent onto Windows and Linux endpoints, build policy rules and profiles, and manage security events and logs creations exceptions and/or Traps management service-provided central response actions including the new Live Terminal capability.

Scope

- **Course level:** Intermediate
- **Course duration:** 2 days
- **Course format:** Combines instructor-facilitated lecture with hands-on labs on Windows and Linux systems
- **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 Partner 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