TRAPS 4.1: DEPLOY AND OPTIMIZE (EDU-285)

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 should prepare the student to deploy Traps in large-scale or complex configurations and optimize its configuration.

Module 1: Scaling Server Infrastructure
- Small site architectures
- Large site architectures
- TLS/SSL deployment considerations

Module 2: Scaling Agent Deployment
- Distributing Traps via GPO
- Configuring Virtual Desktop Infrastructure with Traps

Module 3: ESM Tuning
- Tuning ESM settings
- External logging and SIEM integration
- Role Based Access Control (RBAC)
- Defining Conditions
- Tuning Policies
- Implementing ongoing maintenance

Module 4: Windows migrations for Traps
- SQL database migration
- SSL certificate migration

Module 5: Advanced Traps Forensics
- Best practices for managing forensic data
- Agent queries
- Resources for malicious software testing
- Exploit challenge testing with Metasploit
- Exploit dump analysis with windbg

Module 6: Advanced Traps Troubleshooting
- ESM and Traps architecture
- Troubleshooting scenarios using dbconfig and cytool
- Troubleshooting application compatibility and BITS connectivity

Course Objectives

Students should learn how to design, build, implement, and optimize large-scale Traps deployments: those with multiple servers and/or thousands of endpoints. In hands-on lab exercises, students will distribute Traps endpoint software in an automated way; prepare master images for VDI deployment; build multi-ESM deployments; design and implement customized policies; test Traps with exploits created using Metasploit; and examine prevention dumps with windbg.

Scope

- **Course level:** Intermediate
- **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

Security Engineers, System Administrators, and Technical Support Engineers

Prerequisites

Students should have completed “Traps 4.1: Install, Configure, and Manage” or (for Palo Alto Networks employee and partner SEs) “PSE: Endpoint Associate” training. Windows system administration skills and familiarity with enterprise security concepts also are required.

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