TRAPS 4.0: 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 equips 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 will 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 4.0

Target Audience

Security Engineers, System Administrators, and Technical Support Engineers

Prerequisites

Students should have completed “Traps: 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.

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