TRAPS 4.2: INSTALL, CONFIGURE, AND MANAGE (EDU-181)

Palo Alto Networks Traps™ Advanced Endpoint Protection prevents sophisticated vulnerability exploits and unknown malware-driven attacks. Successful completion of this digital learning course helps prepare students to install on-premises Traps in basic configurations.

Course Modules
1 - Traps Overview
2 - Installing Traps
3 - Malicious Software Overview
4 - Consoles Overview
5 - Traps Protection Against Exploits
6 - Traps Protection Against Malware
7 - Prevention Event Exceptions
8 - Managing Traps
9 - Traps Forensics Capabilities
10 - Basic Traps Troubleshooting
11 - Traps 4.1 and 4.2 What’s New

Scope
- **Level**: Introductory
- **Duration**: 6 hours
- **Format**: Narrated courseware with knowledge check questions
- **Platform support**: Palo Alto Networks Traps Advanced Endpoint Protection ESM 4.2

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 protection from known and unknown malware.

Target Audience
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
The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks Security Operating Platform and your ability to help prevent successful cyberattacks and safely enable application.