Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Traps 4.2: Install Configure & Manage

CODE:	LENGTH:	PRICE:
PAN_EDU-281	16 Hours (2 days)	€1,500.00

Description

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 students to install on-premise Traps in basic configurations.

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.

Audience

Security Engineers, System Administrators, and Technical Support Engineers

Prerequisites

Students must have Windows system administration skills and familiarity with enterprise security concepts.

Programme

Module 1: Traps Overview
• How sophisticated attacks work today
• The design approach of Traps
• Traps components and resources
Module 2: Installing Traps
• Planning the installation
• Installing the ESM Server and Console
• Installing Windows and macOS agents
• Managing content updates
• Upgrading Traps
Module 3: Malicious Software Overview
• Basics of computer architecture
• Exploitation techniques and their prevention
• Malware techniques and their prevention
Module 4: Consoles Overview
• Introduction to the ESM Console
• Introduction to the Traps Agent Console
Module 5: Traps Protection Against Exploits
• Architecture and EPMs
• Configuring exploit protection
Module 6: Traps Protection Against Malware
• Malware protection process flow and components
• Trusted signer management
• Post-detection malware analysis
Module 7: Prevention Event Exceptions
• Prevention events
• Malware/Exploit Protection Module (MPM/EMP) events

• Execution Restriction events
• WildFire® hash control events
• Post-Detection events
Module 8: Managing Traps
• System monitoring
• Traps Server and Agent license administration
• Server settings, users, and roles
• Agent settings and Agent actions
Module 9: Traps Forensics Capabilities
• Forensics workflow and policies
• Responding to prevention events, and logging
Module 10: Basic Traps Troubleshooting
• DIReC methodology and troubleshooting resources
• Working with the technical support
• Troubleshooting installation, connectivity, and upgrades

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

This training is also available as onsite training. Please contact us to find out more.