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: Deploy and Optimize

CODE:	LENGTH:	PRICE:
PAN_EDU-285	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 should prepare the student to deploy on-premise Traps in large-scale or complex configurations and optimize its configuration.

Objectives

Students will learn how to design, build, implement, and optimize largescale 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.

Audience

Security Engineers, System Administrators, and Technical SupportEngineers

Prerequisites

Students should have completed "Traps 4.2: 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. An elementary level of Linux shell experience is needed only for the Linux lab activity.

Programme

Module 1: Scaling Server Infrastructure
• Small site architectures
• Large site architectures
• TLS/SSL deployment considerations
• Installing and configuring the Linux agent
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)
• Virtual groups
• 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

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

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