Updated on 27/05/2024

Sign up

Palo Alto Traps training: deployment and optimization

(EDU-285)

2 days (14 hours)

Presentation

Traps™ Advanced Endpoint Protection from Palo Alto Networks® helps prevent sophisticated exploitation of vulnerabilities, as well as attacks using unknown malware. At the end of this 2-day training course in French, led by a certified instructor, the student participating in this training course will be able to deploy Traps in large infrastructures, and optimize its configuration. Through theory presented by a certified instructor and practical exercises, students will learn how to design, install and optimize Traps deployments on large infrastructures: those with multiple servers and/or thousands of client workstations. Among the practical exercises on offer, students will have the opportunity to automate Traps deployment, prepare images for VDI deployments, deploy multiple servers, design and implement custom policies; test Traps with exploits created by Metasploit; and analyze exploit dumps via Windbg. Our training will be based on the latest version of the tool, PAN-OS 10.1.

Objectives

Install and optimize Traps deployments on large infrastructures

Target audience

Security Engineers, Systems Admins, Support Engineers

Prerequisites

- Students must have completed Traps 281 or PSE: Endpoint Associate training.
"
- Windows administration skills, and knowledge of corporate security concepts are also required

Palo Alto Traps training program: deployment and

optimization

Traps deployment

- Agent distribution
- SSL/TLS deployment options
- Deployment in a VDI context
- External logging and SIEM integration

Traps sizing

- Role-based access control (RBAC)
- Deployment principles, with multiple ESM server options
- Migration principles

Traps optimization

- Optimizing server configuration
- Definition of conditions
- Definition of optimized policies
- Operational maintenance

Post-attack analysis (advanced)

- Agent requests
- Resources for malware testing
- Metasploitt
- Analysis of dump files with windbg

Advanced diagnostics

- Endpoint Security Manager and Traps architectures
- Diagnostic scenarios with dbconfig and cytool
- Application compatibility diagnostics
- BITS connectivity diagnostics

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train its teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.