PAN-EDU-285 - Palo Alto Networks® - Traps: Deploy and Optimize

Palo Alto Networks® - Firewall - Cyber Security

Durata:	Lingue:	Certificazione:
2 Giorni	**Italiano**	**-**

Descrizione del corso

Students should 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.

Programma

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