## PAN-EDU-290 - Palo Alto Networks® - Traps: Cloud Service Operations

Palo Alto Networks® - Firewall - Cyber Security

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

## Descrizione del corso

Students should learn how Traps protects against exploits and malware-driven attacks. In hands-on lab exercises, students will explore and configure new cloud-based Traps Management Service and install Traps endpoint components; build policy rules and profiles; enable and disable process protections; and integrate Traps with Palo Alto Networks WildFire® cloud service, which provides prevention and detection of zero-day malware.

## Programma

**Module 1: Traps Overview**
• How Sophisticated Attacks Work Today
• Traps Multi-Method Threat Prevention
• Traps Components and Resources

**Module 2: Cloud Services**
• Application Framework and Cloud Services Portal
• Shared Services and Traps Onboarding Flow

**Module 3: Cloud- Based Management**
• Traps Service Dashboard and Licensing
• Cross-Platform Agent and Agent Installation
• Endpoints and Endpoint Groups

**Module 4: Policy Rules and Profiles**
• Profiles and Policy Rules
• Agent Settings Profile

**Module 5: Malware Protection Flow**

**ITCore Group**

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
www.itcoregroup.com

- Traps Malware Protection Modules Overview
- Restrictions Profiles, Malware Profiles, and Scanning

**Module 6: Exploits and Exploitation Techniques**

- Application Exploit Prevention
- Exploitation Techniques and Defense Mechanisms
- Basics of Process Management (Optional)

**Module 7: Exploit Protection Modules**

- Architecture and Overview
- Exploit Protection Modules (EPMs)
- Exploit Profiles

**Module 8: Event Management**

- Security Event Logs and Exceptions
- Endpoint and Server Logs
- Manage Quarantined Files

**Module 9: Basic Traps Troubleshooting**

- Troubleshooting Methodology and Resources
- Traps Cytool and Agent Identification
- Traps Agent Log Files and Agent Persist Databases
- Working with Technical Support

**Module 10: Traps Architecture**

- AWS Services Used by Traps Service
- Multi-Regional Architecture
- Agent File Uploads and Downloads
- Agent-Server Communication

**Module 11: Directory Sync Service**

- Directory Sync Service – Activation and Setup
- Troubleshooting