Authorized Training Center

CLICO

paloalto NETWORKS

INCIDENT RESPONSE

PALO ALTO NETWORKS SECURITY

TRAINING OBJECTIVE:

To effectively manage cybersecurity in organizations, professionals need a thorough understanding of how cybercriminals operate, as well as the ability to utilize available tools and security solutions to analyze incidents and respond appropriately. This training is designed to provide IT staff and SOC operators with hands-on experience, enabling them to analyze real-world cyberattacks, assess situations, and respond to incidents effectively.

PRACTICAL EXERCISES:

The training includes practical exercises conducted in a dedicated training environment equipped with Palo Alto Networks security solutions (NGFW, EDR) and individual participant workstations running Kali Linux with the Cyber Soldier Project application. The environment also includes various Web/SMB servers and an Active Directory setup to simulate real-world cyberattacks. Participants will apply techniques commonly used in actual cyberattacks, following the MITRE ATT&CK framework. These techniques include, but are not limited to: OS Credential Dumping: LSASS Memory / Security Account Manager, Web Shell, Exploitation for Privilege Escalation, Lateral Tool Transfer, Pass the Hash and Exploitation of Remote Services.

UNIQUE BENEFITS FOR TRAINING PARTICIPANTS:

Participants will engage with real-world attack techniques encountered in actual cybercriminal activities. They will also gain access to specialized cybersecurity systems, including a Next-Generation Firewall with comprehensive security features and Endpoint Detection and Response (EDR) with live forensics capabilities. These tools will allow participants to observe how effectively specific cyberattack techniques can be detected using advanced security tools. The skills acquired during this training will significantly enhance participant's ability to detect and respond to real-world cyberattacks at an early stage.

DAY 1 INTRODUCTION TO RED TEAM AND ADVERSARY EMULATION

- How does an actual cyber attack work?
- MITRE ATT&CK in real-world cyber attack scenarios
- Introduction to Cyber Range Lab and Cyber Soldier Offensive Tools

PRACTICAL EXERCISES

System Discovery, Reconnaissance, and Sensitive Data Collection

- Basic Offensive Skills Exercise in Cyber Range – Part 1
- Optional: Analyzing traces using tools in Next-Generation Firewall (NGFW) or Network Detection and Response (NDR)
- Scenario - Active Directory Reconnaissance
- Scenario - Network Reconnaissance
- Scenario - Deploying a Web Shell to an Editable SMB Share on a Web Server, Executing Commands on a Windows System
- Analysis of Cyber Attack Traces Using Live Forensics Tools in Endpoint Detection and Response (EDR)
- Optional: Analyzing traces using tools in Next-Generation Firewall (NGFW) or Network Detection and Response (NDR)

DAY 2 PRACTICAL EXERCISES

Password Attacks, Credential Gathering, and Lateral Movement

- Basic Offensive Skills Exercise in Cyber Range – Part 2
- Analysis of Cyber Attack Traces Using Live Forensics Tools Available in Endpoint Detection and Response (EDR)
- Optional: Analyzing traces using tools in Next-Generation Firewall (NGFW) or Network Detection and Response (NDR)
- Scenario - Cracking Service Account Passwords in Windows Domain (Kerberoasting)
- Scenario - Password Spraying Attack on Local Admin Accounts
- Scenario - Windows Credential Dumping using Service Account and Webshell
- Analysis of Cyber Attack Traces Using Live Forensics Tools in Endpoint Detection and Response (EDR)
- Optional: Analyzing traces using tools in Next-Generation Firewall (NGFW) or Network Detection and Response (NDR)

DAY 3 PRACTICAL EXERCISES

Exploitation and Credential Theft, Privilege Escalation

- Exploiting SMB Vulnerabilities on Older Windows Servers – MS17-010 Eternal
- Analysis of Cyber Attack Traces Using Live Forensics Tools Available in Endpoint Detection and Response (EDR)
- Optional: Analyzing traces using tools in Next-Generation Firewall (NGFW) or Network Detection and Response (NDR)
- Scenario - Credential Dumping from SAM Using Admin Password or NTLM Hash
- Scenario - Credential Dumping from LSASS Using Admin Password or NTLM Hash
- Scenario - Lateral Movement to Windows System as Administrator
- Analysis of Cyber Attack Traces Using Live Forensics Tools in Endpoint Detection and Response (EDR)
- Optional: Analyzing traces using tools in Next-Generation Firewall (NGFW) or Network Detection and Response (NDR)

Training price: €950 net per person
(training dates are set individually for groups of min. 4 people)

Authorized Training Center
CLICO

More information:
info@clico.bg
https://clico.bg/trainings »