Authorized Training Center

CLICO

elastic

INCIDENT RESPONSE

WITH ELASTIC SECURITY

TRAINING OBJECTIVES:

The goal of this training is to provide IT and security professionals with **practical skills for effective incident response** using the **Elastic Security platform (SIEM & EDR)**.

Participants learn how to recognize and analyze the actions of cyber adversaries, classify attack techniques according to **MITRE ATT&CK**, and make informed decisions throughout the **Incident Response** process.

The course develops competencies essential for post--incident analysis, threat detection, and incident management in production environments.

PRACTICAL EXERCISES:

The training takes place in a **realistic simulation environment – a Cyber Range built like a real IT system**, including Active Directory and commonly used enterprise services.

Participants perform **step-by-step cyberattack scenarios based on Threat Intelligence**, applying real-world techniques such as Discovery, Privilege Escalation, Credential Dumping, Lateral Movement, and Exploitation of Remote Services.

Each stage of the attack is **monitored in real time through Elastic SIEM and EDR**, allowing participants to understand how attacks are detected, correlated, and analyzed by enterprise-class security systems.

UNIQUE BENEFITS FOR PARTICIPANTS

The Incident Response with Elastic Security training combines cyber range simulations, technical education, and digital forensics into one cohesive learning experience.

1. **Training with digital forensics tools (EDR/ SIEM)**
   Practical exercises using the full capabilities of Elastic Security, including Live Forensics, event detection, and alert correlation.
2. **Cyber Range built like a real IT infrastructure**
   A complete environment with a domain controller, servers, and endpoints, replicating real-world enterprise systems.
3. **Cyberattack scenarios based on Threat Intelligence**
   Simulations inspired by real APT group activities and intelligence-driven incident reports.
4. **Attack scenarios explained and executed using the Cyber Soldier BAS educational platform**
   An interactive introduction to offensive (hacking) techniques.

TRAINING OUTCOME: Participants learn not only how to detect incidents, but also how to understand the logic of the attack and apply incident response methodology effectively — enabling faster detection, accurate analysis, and more efficient mitigation of real-world threats.

Day 1 Basic Offensive Techniques; Active Directory & Network Discovery; Exploitation: Deploying a Web Shell

- Introduction to Red Teaming and Adversary Emulation
- Introduction to Cyber Range Lab and Cyber Soldier Offensive Tools

PRACTICAL HANDS-ON EXERCISES

- Basic Offensive Skills Exercise in Cyber Range – Part 1
- Attack path - Active Directory Reconnaissance
- Attack path - Network Reconnaissance
- Attack path - 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 SIEM and Endpoint Detection and Response (EDR)

Day 2 Credential Access and Lateral Movement

PRACTICAL HANDS-ON EXERCISES

- Basic Offensive Skills Exercise in Cyber Range – Part 2
- Analysis of Cyber Attack Traces Using Live Forensics Tools in SIEM and EDR
- Attack path - Cracking Service Account Passwords in Windows Domain (Kerberoasting)
- Attack path - Password Spraying Attack on Local Admin Accounts
- Attack path - Windows Credential Dumping using Service Account and Web Shell
- Analysis of Cyber Attack Traces Using Live Forensics Tools in SIEM and EDR

Day 3 Aggressive Exploitation; Privilege Escalation, Credential Dumping and Continued Lateral Movement

PRACTICAL HANDS-ON EXERCISES

- Exploiting SMB Vulnerabilities on Older Windows Servers – MS17-010 Eternal
- Analysis of Cyber Attack Traces Using Live Forensics Tools in SIEM and EDR
- Attack path - Credential Dumping from SAM Using Admin Password or NTLM Hash
- Attack path - Credential Dumping from LSASS Using Admin Password or NTLM Hash
- Attack path - Lateral Movement to Windows System as Administrator
- Analysis of Cyber Attack Traces Using Live Forensics Tools in SIEM and EDR

Training price: €950 per person
(training dates are arranged individually for groups of at least 4 participants).

Authorized Training Center
CLICO

More information:
atc@clico.pl
https://clico.pl/trainings »