Autoryzowane Centrum Szkoleniowe CLICO

CHECK POINT

INCIDENT RESPONSE

W ZABEZPIECZENIACH CHECK POINT

CEL SZKOLENIA:

Aby skutecznie zarządzać cyberbezpieczeństwem w organizacjach, specjaliści muszą dokładnie rozumieć sposób działania cyberprzestępców oraz posiadać umiejętność korzystania z dostępnych narzędzi i rozwiązań zabezpieczających w celu analizy incydentów i odpowiedniego reagowania. Szkolenie to zostało zaprojektowane tak, aby zapewnić pracownikom IT i operatorom SOC praktyczne doświadczenie, umożliwiające im analizowanie rzeczywistych cyberataków, ocenę sytuacji oraz skuteczne reagowanie na incydenty.

ĆWICZENIA PRAKTYCZNE:

Szkolenie obejmuje praktyczne ćwiczenia prowadzone w dedykowanej sieci szkoleniowej wyposażonej w zabezpieczenia Check Point (NGFW, EDR) oraz indywidualne stanowiska pracy uczestników z systemem Kali Linux oraz zainstalowaną aplikacją Cyber Soldier Project. W sieci znajdują się również różnego rodzaju serwery Web/SMB oraz środowisko Active Directory, aby w pełni zasymulować rzeczywiste cyberataki. Uczestnicy będą stosować techniki powszechnie wykorzystywane w rzeczywistych cyberatakach, zgodnie z frameworkiem MITRE ATT&CK. Do tych technik należą między innymi: OS Credential Dumping: LSASS Memory / Security Account Manager, Web Shell, Exploitation for Privilege Escalation, Lateral Tool Transfer, Pass the Hash oraz Exploitation of Remote Services.

UNIKALNE KORZYŚCI DLA UCZESTNIKÓW SZKOLENIA:

Uczestnicy zajęć wykonują realne techniki ataków spotykane w rzeczywistych działaniach cyberprzestępców i przy tym posiadają dostęp do specjalistycznych systemów cyberbezpieczeństwa (m.in. Next-Generation Firewall, EDR z narzędziami Live Forensics i Threat Hunting), za pomocą których obserwują w jakim zakresie w rzeczywistości możliwe jest wykrywanie poszczególnych technik cyberataków za pomocą specjalistycznych narzędzi zabezpieczeń. Zdobyte w czasie szkolenia umiejętności w znacznym zakresie pomagają we wczesnym wykrywaniu i obsłudze rzeczywistych cyberataków.

Dzień 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

ĆWICZENIA PRAKTYCZNE

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)

Dzień 2 ĆWICZENIA PRAKTYCZNE

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)

Dzień 3 ĆWICZENIA PRAKTYCZNE

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)

Cena szkolenia: 3900 zł netto od osoby
(terminy szkoleń ustalane są indywidualnie dla grup min. 4 osób)

Autoryzowane Centrum Szkoleniowe CLICO

Więcej informacji:
atc@clico.pl
www.clico.pl »