paloalto NETWORKS

Szkolenie **INCIDENT RESPONSE** w zabezpieczeniach Palo Alto Networks

Incident Response MASTER

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 rzecz wistych cyberataków, ocenę sytuacji oraz skuteczne reagowanie na incydenty.

ĆWICZENIA PRAKTYCZNE:

Szkolenie obejmuje praktyczne ćwiczenia prowadzone w dedykowanej sieci szkoleniowej wyposażonej w zabezpieczenia Palo Alto Networks (NGFW, XDR), a także 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 przez cyberprzestępców, zgodnie z frameworkiem MITRE ATT&CK. Do tych technik należą między innymi: OS Credential Dumping: LSASS Memory / Security Account Manager, Web Shell, Exploitationfor 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 z kompletem funkcjonalności, Endpoint Detection and Response z narzędziami Live Forensics i Threat Hunting). Za pomocą tych systemów uczestnicy 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.

Cyber Range

Autoryzowane Centrum Szkoleniowe CLICO

Dzień 1 WPROWADZENIE DO TEMATYKI RED TEAM ORAZ ADVERSARY EMULATION

- Jak przebiega rzeczywisty cyber atak?
- Techniki i taktyki MITRE ATT&CK na przykładzie prawdziwych cyber ataków.
- Zapoznanie ze środowiskiem Cyber Range i aplikacją Cyber Soldier

ĆWICZENIA PRAKTYCZNE

Rozpoznawanie systemów, Rekonesans, Zbieranie danych wrażliwych

- Podstawowe umiejętności ofensywne - ćwiczenia w Cyber Range – Część 1
- Opcjonalnie: Analiza ruchu za pomocą Next Generation Firewall (NGFW) lub Network Detection and Response (NDR)
- Scenariusz: Active Directory Reconnaissance
- Scenariusz: Network Reconnaissance
- Scenariusz: Deploying a Web Shell to an Editable SMB Share on a Web Server, Executing Commands on a Windows System
- Analiza śladów cyberataku z użyciem narzędzi Live Forensic w ramach Endpoint Detection and Response (EDR)
- Opcjonalnie: Analiza ruchu za pomocą Next Generation Firewall (NGFW) lub Network Detection and Response (NDR)

Dzień 2 ĆWICZENIA PRAKTYCZNE

Ataki na hasła, Zbieranie poświadczeń, "Lateral Movement"

- Podstawowe umiejętności ofensywne - ćwiczenia w Cyber Range – Część 2
- Analiza śladów cyberataku z użyciem narzędzi Live Forensic w ramach Endpoint Detection and Response (EDR)
- Opcjonalnie: Analiza ruchu za pomocą Next Generation Firewall (NGFW) lub Network Detection and Response (NDR)
- Scenariusz: Cracking Service Account Passwords in Windows Domain (Kerberoasting)
- Scenariusz: Password Spraying Attack on Local Admin Accounts
- Scenariusz: Windows Credential Dumping using Service Account and Webshell
- Analiza śladów cyberataku z użyciem narzędzi Live Forensic w ramach Endpoint Detection and Response (EDR)
- Opcjonalnie: Analiza ruchu za pomocą Next Generation Firewall (NGFW) lub Network Detection and Response (NDR)

Dzień 3 ĆWICZENIA PRAKTYCZNE

Exploitacja i kradzież poświadczeń, Eskalacja uprawnień

- Exploitacja podatności SMB na starszych serwerach Windows – MS17 010 Eternal
- Analiza śladów cyberataku z użyciem narzędzi Live Forensic w ramach Endpoint Detection and Response (EDR)
- Opcjonalnie: Analiza ruchu za pomocą Next Generation Firewall (NGFW) lub Network Detection and Response (NDR)
- Scenariusz: Credential Dumping from SAM Using Admin Password or NTLM Hash
- Scenariusz: Credential Dumping from LSASS Using Admin Password or NTLM Hash
- Scenariusz: Lateral Movement to Windows System as Administrator
- Analiza śladów cyberataku z użyciem narzędzi Live Forensic w ramach Endpoint Detection and Response (EDR)
- Opcjonalnie: Analiza ruchu za pomocą Next Generation Firewall (NGFW) lub 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 »