Autoryzowane Centrum Szkoleniowe CLICO

elastic

INCIDENT RESPONSE

Z ELASTIC SECURITY

CELE SZKOLENIA:

Celem szkolenia jest praktyczne przygotowanie specjalistów IT i bezpieczeństwa do **skutecznego reagowania na incydenty cyberbezpieczeństwa** z wykorzystaniem platformy **Elastic Security (SIEM & EDR)**.

Uczestnicy uczą się rozpoznawać i analizować działania cyberprzestępców, klasyfikować techniki wg **MITRE ATT&CK**, oraz podejmować trafne decyzje w procesie Incident Response.

Szkolenie rozwija kompetencje niezbędne do prowadzenia analizy powłamaniowej, wykrywania zagrożeń i zarządzania incydentami w środowiskach produkcyjnych.

ĆWICZENIA PRAKTYCZNE:

Zajęcia odbywają się w realistycznym środowisku symulacyjnym – **Cyber Poligonie zbudowanym jak prawdziwy system informatyczny**, obejmującym Active Directory i najczęściej spotykane usługi IT.

Uczestnicy wykonują krok po kroku **scenariusze cyberataków oparte o Threat Intelligence**, wykorzystując rzeczywiste techniki, takie jak Discovery, Privilege Escalation, Credential Dumping, Lateral Movement czy Exploitation of Remote Services.

Każdy etap ataku jest obserwowany w czasie rzeczywistym w narzędziach **Elastic SIEM i EDR**, co pozwala zrozumieć, jak ataki są wykrywane, korelowane i analizowane przez systemy bezpieczeństwa klasy enterprise.

UNIKALNE KORZYŚCI DLA UCZESTNIKÓW SZKOLENIA:

Szkolenie „Incident Response z Elastic Security" łączy w sobie elementy **cyberpoligonu, edukacji technicznej i informatyki śledczej**.

Uczestnicy zdobywają umiejętności, które można od razu wykorzystać w pracy operacyjnej zespołów SOC, CERT i IT Security.

Najważniejsze wyróżniki szkolenia:

1. **Szkolenie z użyciem narzędzi informatyki śledczej (EDR/SIEM)** – praktyczna praca z pełnym zestawem funkcji Elastic Security, w tym Live Forensics, detekcja zdarzeń i korelacja alertów.
2. **Cyber Poligon zbudowany jak prawdziwy system informatyczny** – pełna infrastruktura IT z kontrolerem domeny, serwerami i stacjami końcowymi, odwzorowująca rzeczywiste środowisko organizacji.
3. **Scenariusze cyberataków oparte o Threat Intelligence** – symulacje inspirowane działaniami faktycznych grup APT i incydentami z raportów wywiadu cybernetycznego.
4. **Scenariusze ataków wyjaśniane i wykonywane z pomocą aplikacji edukacyjnej Cyber Soldier BAS** – interaktywne wprowadzenie do technik ofensywnych (hacking) w kontrolowanym środowisku.

EFEKT SZKOLENIA: Uczestnicy uczą się nie tylko, jak wykrywać incydenty, ale także jak rozumieć logikę ataku i skutecznie stosować metodykę reagowania na incydenty — co umożliwia szybsze wykrywanie, precyzyjniejszą analizę oraz skuteczniejsze ograniczanie rzeczywistych zagrożeń.

Dzień 1 Podstawowe techniki ofensywne; Active Directory i odkrywanie sieci; Eksploatacja: wdrożenie web shella

- Wprowadzenie do Red Teamingu i Adversary Emulation
- Wprowadzenie do laboratorium Cyber Range i narzędzi ofensywnych Cyber Soldier

PRAKTYCZNE ĆWICZENIA WARSZTATOWE

- Ćwiczenie podstawowych umiejętności ofensywnych w Cyber Range – część 1
- Ścieżka ataku – rekonesans Active Directory
- Ścieżka ataku – rekonesans sieciowy
- Ścieżka ataku – wdrożenie web shella na edytowalnym udziale SMB serwera WWW i wykonywanie poleceń na systemie Windows
- Analiza śladów ataku przy użyciu narzędzi Live Forensics w SIEM i Endpoint Detection and Response (EDR)

Dzień 2 Dostęp do poświadczeń i przemieszczanie się w sieci (Lateral Movement)

PRAKTYCZNE ĆWICZENIA WARSZTATOWE

- Ćwiczenie podstawowych umiejętności ofensywnych w Cyber Range – część 2
- Analiza śladów ataku przy użyciu narzędzi Live Forensics w SIEM i EDR
- Ścieżka ataku – łamanie haseł kont usług w domenie Windows (Kerberoasting)
- Ścieżka ataku – atak password spraying na konta lokalnych administratorów
- Ścieżka ataku – zrzucanie poświadczeń w Windows przy użyciu konta usługowego i web shella
- Analiza śladów ataku przy użyciu narzędzi Live Forensics w SIEM i EDR

Dzień 3 Agresywna eksploatacja; eskalacja uprawnień, zrzucanie poświadczeń i kontynuacja przemieszczania się w sieci

PRAKTYCZNE ĆWICZENIA WARSZTATOWE

- Eksploatacja podatności SMB na starszych serwerach Windows – MS17-010 (EternalBlue)
- Analiza śladów ataku przy użyciu narzędzi Live Forensics w SIEM i EDR
- Ścieżka ataku – zrzucanie poświadczeń z SAM przy użyciu hasła administratora lub hasha NTLM
- Ścieżka ataku – zrzucanie poświadczeń z procesu LSASS przy użyciu hasła administratora lub hasha NTLM
- Ścieżka ataku – przemieszczanie się w sieci do systemów Windows jako administrator
- Analiza śladów ataku przy użyciu narzędzi Live Forensics w SIEM i EDR

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

Autoryzowane Centrum Szkoleniowe CLICO

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