Szkolenie

BLUE TEAM - Poziom 2 - Zawansowane bezpieczeństwo infrastruktury. Active Directory. Systemy zabezpieczeń sieciowych

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

To trzecie szkolenie z cyklu Blue Team, skupiające się na zaawansowanych aspektach bezpieczeństwa infrastruktury IT oraz Active Directory. Współczesne sieci korporacyjne są nieustannie narażone na ataki – od prób włamania i eksfiltracji danych po lateral movement i przejęcia kont uprzywilejowanych.

Szkolenie to wyposaży uczestników w wiedzę i umiejętności niezbędne do skutecznej ochrony infrastruktury IT, wykrywania zagrożeń oraz reagowania na incydenty.

Uczestnicy dowiedzą się, jak dbać o bezpieczeństwo Active Directory, skutecznie konfigurować firewalle, IDS/IPS oraz WAF, a także jak zabezpieczać krytyczne tożsamości (IAM, PAM) oraz dane przed wyciekiem (DLP, backup).

Praktyczne laboratoria oparte na realnych zagrożeniach – uczestnicy przeanalizują rzeczywiste przypadki ataków i incydentów bezpieczeństwa, wykorzystując narzędzia na co dzień używane przez specjalistów. Dzięki temu nauczą się stosować skuteczne metody ochrony systemów IT.

Korzyści po szkoleniu

- Zrozumiesz, jak działa Active Directory i jakie są kluczowe zagrożenia
- Nauczysz się skutecznie bronić AD przed atakami
- Opanujesz zaawansowaną konfigurację firewalli, IDS/IPS oraz WAF
- Zdobędziesz umiejętności w zakresie zarządzania tożsamościami i dostępem (IAM, PAM)

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł
Numer NIP: 634-012-60-68, numer REGON: 008173852

- Poznasz strategie ochrony danych przed wyciekiem i backupu odpornego na ransomware
- Będziesz potrafił monitorować incydenty i wykrywać zagrożenia w sieci

Wymagania

- Konieczna wiedza z poziomu 0 i poziomu 1 cyklu Blue Team:
- **BLUE TEAM - Poziom 0 - Wprowadzenie do cyberbezpieczeństwa. Podstawy bezpieczeństwa sieciowego. Narzędzia Windows oraz Linux**
- **BLUE TEAM - Poziom 1 - Analiza Logów i ruchu sieciowego. IT Monitoring & Hardening**

Wiedza wymagana do realizacji kursu:

- Podstawowa znajomość działania Active Directory
- Podstawy administracji systemami Windows/Linux
- Zrozumienie mechanizmów firewalli i sieci TCP/IP
- Znajomość protokołów uwierzytelniania (Kerberos, NTLM)
- Podstawowa wiedza o atakach sieciowych i metodach ich wykrywania

---

Program szkolenia

Moduł 1: Bezpieczeństwo Active Directory

Active Directory jest kluczowym elementem infrastruktury IT, ale także jednym z najczęstszych celów ataków. W tym module uczestnicy poznają mechanizmy działania AD, metody uwierzytelniania (Kerberos, NTLM) oraz popularne techniki ataków, takie jak Pass-the-Hash, Kerberoasting inne. Nauczą się również wdrażać najlepsze praktyki zabezpieczeń, w tym hardening GPO, zarządzać uprawnieniami oraz monitorować logi AD.

- Struktura i mechanizmy AD (LDAP, Kerberos, NTLM)
- Ataki na AD (Pass-the-Hash, Kerberoasting, i inne)
- Obrona i hardening Active Directory (GPO, LAPS, monitorowanie logów)
- LAB

Moduł 2: Firewall, IDS/IPS, WAF & UTM

Skuteczna ochrona sieci wymaga znajomości narzędzi takich jak firewalle, systemy IDS/IPS oraz WAF do ochrony aplikacji webowych. Uczestnicy dowiedzą się, jak analizować ruch sieciowy, tworzyć skuteczne reguły blokowania zagrożeń, a także jak optymalnie

konfigurować rozwiązania UTM do wielowarstwowej ochrony organizacji.

- Konfiguracja firewalli
- IDS/IPS – analiza ruchu i tworzenie oraz tuning reguł
- WAF – zabezpieczenie aplikacji webowych
- UTM – ochrona wielowarstwowa i zarządzanie zagrożeniami
- LAB

Moduł 3: IAM, PAM, DLP & Backup

Tożsamości i dane to jedne z najcenniejszych zasobów organizacji – dlatego wymagają zaawansowanej ochrony. W tym module zaprezentowane zostanie zarządzanie tożsamościami i dostępem (IAM), uprzywilejowanymi kontami (PAM) oraz strategie kontroli dostępu do krytycznych systemów. Uczestnicy nauczą się także zabezpieczać dane przed wyciekiem za pomocą DLP oraz wdrażać skuteczne mechanizmy backupu odporne na ransomware.

- IAM – zarządzanie tożsamościami i dostępem
- PAM – ochrona kont uprzywilejowanych
- DLP – zabezpieczenie przed wyciekiem danych
- Backup i odzyskiwanie danych po ataku ransomware
- DEMO

Tagi:
