Szkolenie

BLUE TEAM - Poziom 3: Detekcja, Reagowanie i Automatyzacja w SOC L1

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie Blue Team Poziom 3 to najbardziej zaawansowany moduł w cyklu edukacyjnym Blue Team. Skierowane jest do specjalistów, którzy opanowali już fundamenty cyberbezpieczeństwa (Poziom 0), logowanie i monitoring (Poziom 1) oraz ochronę infrastruktury (Poziom 2), i chcą wejść na wyższy poziom analizy incydentów, automatyzacji reakcji oraz integracji systemów SOC.

Uczestnicy nauczą się wykorzystywać zaawansowane systemy SIEM i SOAR, analizować alerty bezpieczeństwa w czasie rzeczywistym oraz automatyzować triage i eskalację incydentów. Szczególny nacisk położony jest na **korelację logów**, **detekcję złośliwej aktywności**, analizę wskaźników kompromitacji (IoC) oraz **integrację Threat Intelligence z systemami detekcji**.

Szkolenie opiera się na realistycznych scenariuszach ataków: brute-force, phishing, ransomware oraz APT. Uczestnicy analizują prawdziwe logi z Windows, Linux, firewalli i EDR, wykorzystując narzędzia takie jak **Elastic Stack**, **Shuffle**, **MISP**, **VirusTotal** i inne.

Korzyści po szkoleniu

- Poznanie zaawansowanych funkcji SIEM i korelacji logów.
- Automatyzacja triage alertów i reakcji z wykorzystaniem SOAR.
- Detekcja zaawansowanych zagrożeń (ransomware, phishing, C2).
- Praktyczne wykorzystanie Threat Intelligence w SOC.
- Eskalacja i tworzenie dokumentacji incydentów zgodnie z dobrymi praktykami.

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
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Wymagania

- Konieczna wiedza z poziomu 0-2 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
  - BLUE TEAM - Poziom 2 - Zawansowane bezpieczeństwo infrastruktury. Active Directory. Systemy zabezpieczeń sieciowych

---

Program szkolenia

Moduł 1: SIEM – Analiza logów i alertów

- Wprowadzenie do funkcji SIEM i jego architektury
- Rola SIEM w SOC L1.
- Źródła logów: Windows Event Logs, Sysmon, firewall.
- Ćwiczenia: analiza i korelacja zdarzeń z logów na przykładzie ataków.

Moduł 2: Frameworki detekcji – MITRE ATT&CK, Sigma, YARA

- Rola frameworków w detekcji zagrożeń.
- Łączenie frameworków w SOC L1.
- Proces detekcja zagrożeń.

Moduł 3: Eskalacja alertów i triage, Incident Response (IR)

- 5-punktowa checklista L1 do oceny alertu.
- Tworzenie raportu eskalacyjnego do L2/L3.
- Automatyzacja: auto-close, auto-escalate, tagging, playbooki.
- Etapy reagowania na incydent (wg NIST).
- Ćwiczenia: reakcja na incydent oraz dopasowanie reguł i tworzenie raportu

Moduł 4: SOAR – Automatyzacja reakcji

- Architektura SOAR (Shuffle): webhooki, playbooki, konektory.
- Scenariusze automatyzacji: phishing, ransomware, hash checking.
- Integracja z Elastic, VirusTotal, HybridAnalysis.

Moduł 5: Threat Intelligence – analiza IoC

- TI jako źródło kontekstu: hash, IP, domena, sandbox.
- Narzędzia: VirusTotal, OTX, HybridAnalysis, Any.Run, MISP.
- Korelacja IoC w SIEM (Indicator Match), feedy TI w SOAR.

Tagi:

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
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.