

Szkolenie

BLUE TEAM - Advanced Level - zarządzanie rozwiązaniem SIEM

[Strona szkolenia](#) | [Terminy szkolenia](#) | [Rejestracja na szkolenie](#) | [Promocje](#)

Opis szkolenia

Szkolenie skierowane jest do osób chcących rozwijać swoją karierę w branży cybersecurity. Jest to trzecie szkolenie z cyklu dotyczącego cyberbezpieczeństwa defensywnego prowadzonego przez specjalistów BLUE TEAM.

Szkolenie pozwala na zdobycie wiedzy i umiejętności niezbędnych do pracy w zespole Blue Team Security. Podczas szkolenia zapoznasz się z rozwiązaniem SIEM (Security Information and Event Management) i zrozumiesz jego znaczenie w kontekście cyberbezpieczeństwa. Poznasz funkcjonalności poszczególnych modułów, a dzięki warsztatowej części szkolenia nauczysz się jak efektywnie wykorzystywać jego możliwości podczas symulowanego ataku.

Korzyści po szkoleniu

- niezbędna wiedza techniczna oraz umiejętności pozwalające na rozpoczęcie pracy w zespole Blue Team,
- szkolenie kończy się egzaminem - osoby, które zdadzą pomyślnie test, otrzymają Certyfikat Autoryzowanego Centrum Szkoleniowego DAGMA.

Wymagania

- znajomość podstawowych zagadnień informatycznych (sieci komputerowe, systemy operacyjne) oraz podstaw zarządzania logami w cyberbezpieczeństwie
- zainteresowanie cyberbezpieczeństwem
- zalecane ukończenie szkoleń:
 - [BLUE TEAM - Entry Level - Podstawy zarządzania logami w cyberbezpieczeństwie](#)
 - [BLUE TEAM - Mid Level - praca w zespole Blue Team Security](#)

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

Program szkolenia

Moduł 1: Wprowadzenie do SIEM

- Omówienie Security Information and Event Management
- Znaczenie SIEM w kontekście cyberbezpieczeństwa
- Najważniejsze cechy i funkcje SIEM

Moduł 2: Dane gromadzone przez SIEM

- Źródła danych dla SIEM
- Wymagania ilościowe i jakościowe

Moduł 3: Analiza danych

- Sposoby analizy danych w SIEM
- Identyfikacja zagrożenia
- Wykrywanie anomalii
- Narzędzie i metody analizy danych

Moduł 4: Raportowanie i reagowanie

- Raporty w SIEM
- Możliwe sposoby reakcji na detekcje
- Blokowanie ruchu sieciowego
- Automatyczne reakcje

Moduł 5: Integracja pomiędzy systemami bezpieczeństwa

- Sposoby integrowania systemów w SIEM
- Korzyści z integracji

Moduł 6: Warsztat praktyczny

- Prezentacja symulowanego ataku
- Omówienie systemu SIEM wykorzystywanego w ćwiczeniu
- Analiza zidentyfikowanego zagrożenia
- Omówienie detekcji
- Raport stworzony przez analityka w SOC

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

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
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł
Numer NIP: 634-012-60-68, numer REGON: 008173852