Szkolenie

BLUE TEAM - Poziom 1 - Analiza Logów i ruchu sieciowego. IT Monitoring & Hardening

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie Blue Team Poziom 1 to kontynuacja cyklu szkoleń BLUE TEAM.

Jest to drugie szkolenie z cyklu cyberbezpieczeństwo defensywne, prowadzone przez doświadczonych inżynierów Dagma Blue Team.

Szkolenie obejmuje szczegółowe omówienie mechanizmów rejestrowania zdarzeń oraz sposoby identyfikacji istotnych informacji w logach - zarówno w systemie Windows, jak i Linux. Uczestnicy nauczą się, jak analizować wpisy dotyczące aktywności użytkowników i procesów, co pozwala wykrywać podejrzane aktywności mogące świadczyć o zagrożeniu.

Kolejnym kluczowym elementem jest **analiza ruchu sieciowego**. Uczestnicy dowiedzą się, jak wygląda standardowy ruch w infrastrukturze IT oraz jakie anomalie mogą wskazywać na potencjalne ataki lub naruszenia bezpieczeństwa. Omówione zostaną sposoby monitorowania komunikacji sieciowej, identyfikowania nietypowych zachowań oraz rozpoznawania prób nieautoryzowanego dostępu.

Podczas szkolenia zaprezentowane będą również podstawowe zasady hardeningu w IT, co pozwoli **zabezpieczać systemy i usługi**. Uczestnicy poznają także podstawy pracy z oprogramowaniem typu AV oraz EDR oraz dowiedzą się, jak wykorzystywać te informacje do skutecznego reagowania na incydenty.

Uczestnictwo w szkoleniu pozwoli zdobyć praktyczną wiedzę i umiejętności podczas laboratoriów praktycznych, koncentrujących się na monitorowaniu systemów, analizie ruchu

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.

sieciowego i wzmacnianiu bezpieczeństwa infrastruktury IT. Dzięki połączeniu teorii z praktycznymi przykładami uczestnicy zrozumieją, jak skutecznie identyfikować i analizować zagrożenia, a także jak wspierać działania zespołów odpowiedzialnych za bezpieczeństwo IT.

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

- **Praktyczne umiejętności** – analiza logów, monitorowania systemów i wykrywania zagrożeń w rzeczywistych scenariuszach.
- **Wiedza o monitorowaniu ruchu sieciowego** – identyfikacja anomalii w sieci i rozróżnianie normalnego oraz podejrzanego ruchu.
- **Podstawy hardeningu** – nauka zabezpieczania systemów operacyjnych i usług przed atakami.
- **Świadomość zagrożeń i ataków** – lepsze zrozumienie metod wykorzystywanych przez cyberprzestępców i sposoby ich neutralizacji.
- **Praca z narzędziami wykorzystywanymi przez Blue Team** – praktyczne ćwiczenia z wykorzystaniem narzędzi do monitorowania i analizy bezpieczeństwa.
- **Praca z AV i EDR** – nauka interpretacji zdarzeń rejestrowanych przez oprogramowanie antywirusowe oraz identyfikacji potencjalnych zagrożeń.

Wymagania

- **Podstawowa znajomość systemu operacyjnego** – umiejętność pracy z systemami operacyjnymi Windows i Linux (praca w terminalu) na poziomie podstawowym.
- **Znajomość podstawowych pojęć związanych z IT** – zrozumienie terminologii informatycznej oraz podstaw działania sieci komputerowych.
- **Podstawowa wiedza o bezpieczeństwie IT** – chociaż nie jest to wymagane, ogólne pojęcie o zagrożeniach w sieci oraz ochronie danych będzie przydatne.
- **Podstawowa znajomość pracy z wierszem poleceń** – przydatne będą umiejętności pracy z terminalem (np. PowerShell, CMD w Windows, terminal w Linux) oraz podstawowe komendy systemowe.
- **Dostęp do laptopa/komputera** – w celu realizacji ćwiczeń praktycznych wymagane jest posiadanie własnego sprzętu komputerowego z dostępem do Internetu.

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.

Program szkolenia

Moduł 1: Wprowadzenie

- Znaczenie monitorowania systemów informatycznych
- Logi w kontekście cyberbezpieczeństwa
- Wykrywanie nieautoryzowanego dostępu
- Monitorowanie aplikacji
- Reakcje na zdarzenia

Moduł 2: Windows – Monitorowanie i analiza logów

- Wprowadzenie do systemu Windows w kontekście bezpieczeństwa
- Monitorowanie aktywności użytkowników i aplikacji w systemie Windows
- Analiza logów w Windows Event Viewer: Security Logs, Application Logs
- Podstawowe komendy systemowe, cmd & powershell
- Analiza zdarzeń związanych z bezpieczeństwem
- Lab

Moduł 3: Linux – Monitorowanie i analiza logów

- Wprowadzenie do systemu Linux z perspektywy bezpieczeństwa
- Analiza podstawowych logów systemowych: /var/log/auth.log, /var/log/syslog
- Monitorowanie działań użytkowników w systemie Linux
- Podstawowe komendy systemowe i narzędzia analityczne w Linuxie
- Lab

Moduł 4: Hardening systemów

- Wprowadzenie do hardeningu systemów Windows i Linux
- Zasady zabezpieczania systemów operacyjnych i usług
- Podstawowe komendy sieciowe (ping, tracert, nslookup, netstat, tcpdump i inne).
- Analiza ruchu sieciowego - Wireshark
- Najlepsze praktyki w zakresie zabezpieczania systemów przed atakami
- Lab

Moduł 5: AV/EDR – Analiza logów i wykrywanie zagrożeń

- Wprowadzenie do ESET Inspect jako narzędzia EDR (Endpoint Detection and Response)
- Analiza logów z ESET Inspect: wykrywanie podejrzanych działań
- Interpretacja zdarzeń bezpieczeństwa w logach antywirusowych
- Praktyczne ćwiczenia w analizie logów ESET i identyfikacji zagrożeń

- Demo

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.