Szkolenie

BLUE TEAM - Poziom 0 - Wprowadzenie do cyberbezpieczeństwa. Podstawy bezpieczeństwa sieciowego. Narzędzia Windows oraz Linux

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie „Wprowadzenie do cyberbezpieczeństwa” to doskonały punkt startowy dla osób chcących rozpocząć swoją karierę w branży cybersecurity. Jest to pierwszy kurs z cyklu cyberbezpieczeństwo defensywne, prowadzone przez doświadczonych inżynierów Dagma Blue Team.

Zaprojektowaliśmy to szkolenie z myślą o osobach, które chcą rozpocząć swoją przygodę z cyberbezpieczeństwem, zdobywając solidne podstawy niezbędne do pracy w obszarze ochrony sieci i infrastruktury IT. Wiedza ta jest przydatna zarówno przy realizacji testów penetracyjnych (Offensive Security) jak i analizie, wykrywaniu i mitygacji cyberzabrożeń (Defensive Security).

Uczestnicy poznają podstawowe zasady i narzędzia wykorzystywane w pracy w zespołach BLUE TEAM i SOC (Security Operation Center). Dzięki starannie zaprojektowanym modułom, uczestnicy zdobędą umiejętności, które pozwolą im skutecznie identyfikować, analizować oraz zarządzać zagrożeniami w sieci.

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.

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.

Korzyści

- **Solidne podstawy w cyberbezpieczeństwie** – Uczestnicy zdobędą fundamentalną wiedzę na temat bezpieczeństwa IT, która stanowi podstawę do dalszego rozwoju w tej dziedzinie.
- **Znajomość kluczowych usług sieciowych** – Nabycie umiejętności w zakresie identyfikacji podstawowych portów, usług i protokołów sieciowych, co pozwala na skuteczne zabezpieczanie infrastruktury IT.
- **Praktyczne umiejętności z zakresu narzędzi i komend** – Uczestnicy nauczą się korzystać z narzędzi oraz komend w systemach Windows i Linux, co pozwala na lepsze wykrywanie zagrożeń i zarządzanie bezpieczeństwem systemów.
- **Znajomość wirtualizacji** – Uczestnicy dowiedzą się, jak wykorzystać maszyny wirtualne do testów penetracyjnych, zarządzania infrastrukturą i tworzenia bezpiecznych środowisk testowych.
- **Lepsze przygotowanie do certyfikacji** – Szkolenie stanowi solidny punkt wyjścia do uzyskania certyfikatów z zakresu bezpieczeństwa IT, co zwiększa szanse na rozwój kariery w tej branży.
- **Zwiększenie kompetencji w zakresie bezpieczeństwa IT** – Uczestnicy nabędą praktyczne umiejętności wykorzystywane przez specjalistów ds. bezpieczeństwa IT w codziennej pracy, co zwiększa ich wartość na rynku pracy.
- **Przygotowanie do pracy w zespole Blue Team** – Szkolenie pomoże uczestnikom zrozumieć, jak funkcjonują zespoły zajmujące się ochroną przed cyberzagrożeniami, co umożliwia efektywne działanie w obszarze zarządzania bezpieczeństwem IT.

Wymagania

- Podstawowa umiejętność obsługi komputera – Uczestnicy powinni umieć korzystać z podstawowych aplikacji komputerowych, takich jak przeglądarki internetowe, edytory tekstów.
- Brak konieczności doświadczenia w cyberbezpieczeństwie – Szkolenie jest skierowane zarówno do osób bez doświadczenia w obszarze bezpieczeństwa IT, jak i do tych, którzy chcą poszerzyć swoją wiedzę na ten temat.
- Dostęp do komputera z systemem Windows wraz z Internetem.
- Chęć nauki i zaangażowanie w szkolenie – Uczestnicy powinni być zmotywowani do nauki i aktywnego uczestnictwa w zajęciach oraz ćwiczeniach praktycznych.
- Szkolenie jest zaprojektowane w sposób przyjazny dla początkujących, więc nie jest wymagane zaawansowane doświadczenie w IT.

Program szkolenia

Moduł 1 – Wprowadzenie do cyberbezpieczeństwa

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.

Pierwszy moduł wprowadza uczestników w świat cyberbezpieczeństwa. Uczestnicy zapoznają się z najważniejszymi certyfikacjami, ścieżkami rozwoju zawodowego oraz umiejętnościami niezbędnymi do pracy w tym dynamicznie rozwijającym się obszarze. Dowiedzą się, jakie są aktualne wymagania rynkowe, co pozwala na lepsze zaplanowanie własnej kariery.

- Wprowadzenie do cyberbezpieczeństwa defensywnego i roli Blue Team w IT
- Roadmapa
- Certyfikacje
- Ścieżki rozwoju
- Kompetencje i wiedza, które są wymagane na rynku

Moduł 2 – Podstawowe usługi sieciowe: porty, usługi, protokoły

W tym module uczestnicy poznają kluczowe elementy infrastruktury sieciowej. Omówione zostaną podstawowe porty, protokoły oraz usługi sieciowe, które są fundamentem działania każdego systemu komputerowego. Celem tego modułu jest zrozumienie, jak działa sieć komputerowa oraz jak zabezpieczać poszczególne jej elementy. W części praktycznej uczestnik pozna wcześniej omówione porty, usługi, protokoły w realnej (i podatnej na ataki) infrastrukturze sieciowej, co pozwoli spojrzeć na podstawy bezpieczeństwa IT od strony praktycznej.

- Omówienie protokołów takich, jak HTTP, HTTPS, FTP, SMB, RDP i inne
- Przedstawienie podstawowych portów, które są kluczowe w kontekście bezpieczeństwa sieci
- Prezentacja podstaw sieci: IP, subnetting, NAT, DNS, DHCP, VPN i inne
- Laboratoria praktyczne – skanowanie i analiza usług, portów - środowisko testowe

Moduł 3 – Narzędzia i Komendy w Windows oraz Linux

Moduł ten prezentuje praktyczne zastosowanie komend i narzędzi wykorzystywanych w pracy specjalisty ds. bezpieczeństwa. Uczestnicy poznają komendy i narzędzia zarówno w systemie Windows, jak i Linux, które są niezbędne do codziennej pracy przy monitorowaniu i audytach bezpieczeństwa. W ramach tego modułu omówione zostaną również praktyczne przykłady wykorzystania narzędzi w celu wykrywania luk w zabezpieczeniach usług w wirtualnym środowisku podczas zajęć praktycznych.

- Uczestnicy nauczą się korzystać z terminala w obu systemach operacyjnych, poznając komendy wykorzystywane do monitorowania, analizy i testów bezpieczeństwa.
- Zaprezentowane zostaną przydatne narzędzia do testowania bezpieczeństwa zarówno pod

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.

Windows, jak i Linux.
- Zajęcia obejmują również ćwiczenia praktyczne, w których uczestnicy będą mieli okazję analizować luki w zabezpieczeniach usług oraz nauczyć się, jak sprawdzać ich stan w systemie operacyjnym.

Moduł 4 – Wirtualizacja: zastosowanie maszyn wirtualnych w bezpieczeństwie

Wirtualizacja to jeden z kluczowych elementów nowoczesnego podejścia do zabezpieczeń. Uczestnicy dowiedzą się, jak wykorzystać maszyny wirtualne do tworzenia bezpiecznych środowisk testowych oraz jak zarządzać i kontrolować infrastrukturę wirtualną. Wirtualne maszyny stanowią doskonałą metodę w testach penetracyjnych oraz w tworzeniu izolowanych środowisk do analizy zagrożeń.

- Uczestnicy poznają podstawy wirtualizacji, dowiadując się, czym są maszyny wirtualne (VM) i jak mogą być wykorzystywane w kontekście bezpieczeństwa IT.
- Moduł ten obejmuje teorię oraz praktyczne zastosowania wirtualizacji w zarządzaniu infrastrukturą oraz tworzeniu izolowanych środowisk do analizy zagrożeń.
- Uczestnicy będą mieli okazję stworzyć i zarządzać maszynami wirtualnymi, co pozwoli im na praktyczne wykorzystanie tej technologii w kontekście bezpieczeństwa IT.

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.