Szkolenie

Cisco CyberOps Associate

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Uczestnicy szkolenia zdobędą podstawowe zdolności w obszarze analizy bezpieczeństwa IT tj. podstawową wiedzę niezbędną do skutecznego wykrywania, analizy oraz eskalacji podstawowych zagrożeń cyberbezpieczeństwa przy wykorzystaniu popularnych narzędzi typu open-source.

Egzamin: Treści omawiane w trakcie kursu są dostosowane do wymogów egzaminu 200-201 CBROPS, którego pozytywne zaliczenie jest niezbędne do uzyskania certyfikatu the Cisco Certified CyberOps Associate.

Szkolenie jest prowadzone w języku polskim, materiały są w języku angielskim.

Korzyści

Szkolenia szczególnie dedykowane dla specjalistów IT, którzy chcieli by rozwijać swoją karierę w zespołach Security Operation Center (SOC). Po ukończeniu szkolenia kursanci będą umieli:

- instalować maszyny wirtualne, które pozwolą na implementację i analizę zagrożeń cyberbezpieczeństwa w odizolowanym środowisku,
- wytłumaczyć rolę jaką w organizacji pełni analityk systemów cyberbezpieczeństwa,
- opisać dostępne w systemie Windows funkcjonalności pomocne w prowadzeniu analizy zagrożeń cyberbezpieczeństwa,
- opisać funkcjonalności dostępne w Linuxie,
- przeanalizować działanie protokołów i usług sieciowych,
- wyjaśnić działanie infrastruktury sieciowej,

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.

- sklasyfikować różne rodzaje ataków sieciowych,
- wykorzystywać narzędzia do monitorowania sieci przy identyfikacji ataków na protokoły i usługi sieciowe,
- wytłumaczyć w jaki sposób zablokować niechciany dostęp do sieci komputerowej, hostów i danych,
- wyjaśnić znaczenie kryptografii w procesie monitorowania bezpieczeństwa sieci,
- wytłumaczyć w jaki sposób monitorować podatności i ataki na końcówkach,
- oceniać alerty dotyczące bezpieczeństwa sieci,
- analizować dane z ataków występujących w sieci w celu wykrycia zagrożonych hostów i istniejących podatności,
- zastosować modele reakcji na incydenty w celu zarządzania incydentami związanymi z bezpieczeństwem sieci.

Wymagania

Podstawowa znajomość elementów sieci komputerowej.

Harmonogram szkolenia

- Wstęp / Course Introduction/The Danger
- Cyberprzestępczość / Fighters in the War Against Cybercrime
- Windows / The Windows Operating System
- Linux / Linux Overview
- Protokoły sieciowe / Network Protocols
- Protokoły IP / Ethernet and Internet Protocol (IP)
- Podstawowe zasady bezpieczeństwa sieciowego / Principles of Network Security
- Protokół rozpoznawania adresów / Address Resolution Protocol
- Warstwa transportowa / The Transport Layer
- Usługi sieciowe / Network Services
- Urządzenia komunikacji sieciowej / Network Communication Devices
- Infrastruktura bezpieczeństwa sieci / Network Security Infrastructure
- Narzędzia hackerskie / Attackers and Their Tools
- Typowe zagrożenia i ataki / Common Threats and Attacks
- Obserwowanie działania sieci / Observing Network Operation
- Rodzaje ataków / Attacking the Foundation / Attacking What We Do
- Obrona / Understanding Defense
- Kontrola dostępu / Access Control
- Analiza zagrożeń / Threat Intelligence
- Kryptografia / Cryptography
- Ochrona / Endpoint Protection
- Ocena podatności / Endpoint Vulnerability Assessment

- Technologie i protokoły / Technologies and Protocols
- Dane dotyczące bezpieczeństwa sieci / Network Security Data
- Alerty / Evaluating Alerts
- Praca z danymi bezpieczeństwa sieci / Working with Network Security Data
- Informatyka śledcza, analiza i reagowanie na incydenty / Digital Forensics and Incident Analysis and Response

---

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.