kod szkolenia: CBROPS / PL DL 5d

Understanding Cisco Cybersecurity Operations Fundamentals v 1.1

Szkolenie autoryzwoane Cisco - **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)** nauczy Cię podstawowych pojęć związanych z:

- bezpieczeństwem,
- powszechne operacje i ataki w sieci oraz aplikacjach,
- a także rodzajów danych potrzebnych do badania incydentów bezpieczeństwa.

Szkolenie to pomoże Ci nauczyć się, jak monitorować alerty i naruszenia, a także jak rozumieć i przestrzegać ustalonych procedur reagowania na alerty, które zostały przekształcone w incydenty.

Dzięki połączeniu wykładów, ćwiczeń praktycznych i samodzielnej nauki, poznasz niezbędne umiejętności, pojęcia i technologie, aby stać się wartościowym członkiem Cybersecurity Operations Center (SOC), w tym zrozumienie infrastruktury IT, operacji oraz podatności.

To szkolenie pomoże Ci przygotować się do certyfikacji Cisco® Certified CyberOps Associate oraz roli analityka operacji cyberbezpieczeństwa na poziomie Junior lub Entry-level w SOC. Szkolenie to umożliwia również zdobycie 30 punktów kredytowych (CE) na potrzeby recertyfikacji.

Płać punktami CLC:

Cisco Learning Credits accepted : 43 Credits per Class

Szczegóły i zapisy na stronie dostawcy:

https://learninglocator.cloudapps.cisco.com/#/home

Program Cisco Continuing Education to elastyczna oferta dedykowana dla wszystkich aktywnych osób posiadających certyfikaty na poziomie Associate, Specialist, Professional i Expert.

Dowiedz się więcej, jak możesz recertyfikować się w ramach CE, aby zachować aktywny status certyfikacji.

Cisco Continuing Education Program - CE

Uczestnictwo w autoryzowanym szkoleniu pozwala Ci uzyskać dodatkowe punkty potrzebne do utrzymania certyfikacji.

CBROPS: 30 punktów CE

Odbiorcy szkolenia

Szkolenie dla osób rozpoczynających bądź rozwijających karierę na stanowisku Analityka ds. Cyberbezpieczeństwa w Centrum Bezpieczeństwa Cybernetycznego (SOC). profesjonalistów IT pragnących zdobyć wiedzę na temat operacji związanych z cyberbezpieczeństwem lub osób dążących do uzyskania certyfikatu Cisco Certified CyberOps Associate.

Korzyści

- Szkolenie CBROPS wprowadza uczestników w tematykę infrastruktury teleinformatycznej, jej funkcjonowania oraz podatności związanymi z protokołami używanymi w sieciach TCP/IP.
- Słuchacz pozna podstawowe koncepcje bezpieczeństwa teleinformatycznego i zrozumie działanie typowych aplikacji stosowanych we współczesnych sieciach.
- Zapozna się z typami oraz rodzajami ataków na systemy z rodziny Windows oraz Linux.
- Będzie umiał rozpoznać i sklasyfikować rodzaj incydentu na podstawie próbek przechwyconego ruchu sieciowego oraz analizy systemowych dzienników zdarzeń.
- Słuchacz dowie się w jaki sposób działa Centrum Operacji Cybernetycznych, pozna narzędzia oraz metodologię analizy incydentów.
- Uczestnik zapozna się z typowymi wektorami ataków na sieć komputerową oraz nauczy się identyfikować i obsługiwać incydenty teleinformatyczne.
- Zapozna się z zadaniami stawianymi przed członkami zespołu ds. reagowania na incydenty

komputerowe.

Program szkolenia

1. Wprowadzenie do SOC
   - Definicja i charakterystyka SOC
   - Przegląd narzędzi do analizy ruchu sieciowego
   - Metodologia analizy incydentu w SOC
   - Narzędzia i serwisy do analizy zagrożeń cybernetycznych
2. Analiza incydentów bezpieczeństwa teleinformatycznego
   - Korelacje zdarzeń oraz normalizacja
   - Identyfikacja typowych wektorów ataków na sieć teleinformatyczną
   - Identyfikacja złośliwej aktywności atakującego
   - Identyfikacja incydentów na bazie wzorców oraz odbiegającego od normy działania hosta
   - Obsługa incydentu w sieci teleinformatycznej
3. Protokoły warstwy aplikacji oraz bezpieczeństwo stacji końcowych
   - Podstawy bezpieczeństwa informacyjnego
   - Charakterystyka typowych aplikacji i protokołów L7
   - Koncepcje typowych ataków na warstwę aplikacji
   - Typowe ataki na stacje końcowe działające pod systemem operacyjnym Windwos/Linux
   - Urządzenia instalowane na poziomie sieci do ochrony przez atakami
   - Mechanizmy ochrony stacji końcowych instalowane na poziomie systemu operacyjnego
4. Monitorowanie i analiza incydentów teleinformatycznych
   - Zapoznanie z informacjami zapisywanymi w dziennikach zdarzeń
   - Wprowadzenie do analizy incydentów teleinformatycznych
5. Charakterystyka działania SOC
   - Charakterystyka „SOC Playbook”
   - Charakterystyka „SOC Metrics”
   - Automatyzacja wykrywania incydentów w SOC
   - Plan reagowania na incydenty komputerowe
   - Opis zadań członków zespołu ds. reagowania na incydenty komputerowe
6. Tematyka uzupełniająca (nauka własna)
   - Wprowadzenie do systemu VERIS
   - Charakterystyka działania systemu operacyjnego z rodziny Windows
   - Charakterystyka działania systemu operacyjnego z rodziny Linux
7. Tematyka ćwiczeń laboratoryjnych:
   - Discovery 1: Use NSM Tools to Analyze Data Categories
   - Discovery 2: Explore Cryptographic Technologies
   - Discovery 3: Explore TCP/IP Attacks

- Discovery 4: Explore Endpoint Security
- Discovery 5: Investigate Hacker Methodology
- Discovery 6: Hunt Malicious Traffic
- Discovery 7: Correlate Event Logs, PCAPs, and Alerts of an Attack
- Discovery 8: Investigate Browser-Based Attacks
- Discovery 9: Analyze Suspicious DNS Activity
- Discovery 10: Explore Security Data for Analysis
- Discovery 11: Investigate Suspicious Activity Using Security Onion
- Discovery 12: Investigate Advanced Persistent Threats
- Discovery 13: Explore SOC Playbooks

8. Ćwiczenia do samodzielnej realizacji (poza salą szkoleniową)
   - Discovery 14: Explore the Windows Operating System
   - Discovery 15: Explore the Linux Operating System

Oczekiwane przygotowanie uczestnika

- Wiedza na poziomie kursu CCNA
- Znajomość sieci Ethernet i TCP/IP
- Praktyczna znajomość systemu Windows
- Praktyczna znajomość systemu Linux

Szkolenie obejmuje

- 5 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Autoryzowany podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Język

- Szkolenie: polski
- Materiały: angielski

Metoda egzaminacyjna

Egzamin 200-201 CBROPS
Czas trwania: 120 minut
Egzamin CBROPS sprawdza wiedzę i umiejętności kandydata w zakresie pojęć związanych z:

- security concepts,
- security monitoring,
- host-based analysis,
- network intrusion analysis
- polityk i procedur bezpieczeństwa.

Czas trwania

5 dni / 35 godzin

Opis egzaminu

Szkolenie przygotowuje do egzaminu 200-201 CBROPS, który można zdawać za dodatkową opłata w centrum PearsonVUE. Egzamin można również zdawać w formule on-line. Szczegóły dostępne są na stronie: https://home.pearsonvue.com/cisco/onvue