

kod szkolenia: CBROPS / PL AA 5d

Understanding Cisco Cybersecurity Operations Fundamentals

Szkolenie autoryzowane Cisco.

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



Przeznaczenie szkolenia

Szkolenie dla osób rozpoczynających bądź rozwijających karierę na stanowisku Analityka ds. Cyberbezpieczeństwa w Centrum Bezpieczeństwa Cybernetycznego (SOC).



Korzyści wynikające z ukończenia szkolenia

- 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.



Opis egzaminu

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



Oczekiwane przygotowanie słuchaczy

- Wiedza na poziomie kursu CCNA
- Znajomość systemów z rodziny Windows (preferowane posiadanie certyfikatu MCSA, MCSE)
- Znajomość systemów z rodziny Linux (preferowane posiadanie certyfikatu RHCSA, RHCE, LPI)



Język szkolenia

- Szkolenie: polski
- Materiały: angielski



Czas trwania

5 dni / 35 godzin

Agenda 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 przed 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