

kod szkolenia: SCOR / PL AA 5d

Implementing and Operating Cisco Security Core Technologies



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.

SCOR: 64 punkty CE



Przeznaczenie szkolenia

Szkolenie dla osób zamierzających zabezpieczać sieci komputerowe oparte na rozwiązaniach Cisco w obszarach związanych z przełączaniem, routingiem, dostępem do Internetu oraz ochroną treści serwerów www i e-mail.



Korzyści wynikające z ukończenia szkolenia

Szkolenie SCOR pomaga przygotować się do certyfikacji Cisco® CCNP® Security i CCIE® Security oraz do pracy na stanowisku starszego inżyniera bezpieczeństwa teleinformatycznego.

Na kursie opanujesz umiejętności i technologie potrzebne do wdrożenia podstawowych rozwiązań bezpieczeństwa Cisco, aby zapewnić zaawansowaną ochronę przed atakami cybernetycznymi. Nauczysz się konfigurować bezpieczne sieci, chmury i treści oraz wdrażać ochronę punktów końcowych, konfigurować bezpieczny dostęp do sieci, widoczność użytkowników i egzekwować kontrolę dostępu. Dowiesz się jak wdrażać zaporę Cisco ASA oraz Firepower. Poprzez pokazy instruktorskie na żywo, uczestnicy poznają metodykę oraz specyfikę konfiguracji przełącznika, routera oraz zapory sieciowej Cisco ASA w wymienionym zakresie. Ćwiczenia do samodzielnej realizacji pozwolą na utrwalenie zdobytej wiedzy.



Metoda egzaminowania

Szkolenie przygotowuje do egzaminu 350-701 SCOR, 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>



Opis egzaminu

Szkolenie przygotowuje do egzaminu 350-701 SCOR, 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 kursów ICND1 i ICND2 lub CCNAX lub CCNA.
Wiedza na poziomie kursu SFNDU.



Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Czas trwania

5 dni / 35 godzin

Agenda szkolenia

1. Dzień pierwszy

- Charakterystyka mechanizmów zabezpieczających infrastrukturę teleinformatyczną przed atakami
- Wdrożenie zapory sieciowej na bazie produktu Cisco ASA

2. Dzień drugi

- Wdrożenie zapory sieciowej nowej generacji na bazie rozwiązania Cisco FirePower

3. Dzień trzeci

- Wdrożenie ochrony wiadomości poczty elektronicznej na bazie produktu Cisco Email Content Security

4. Dzień czwarty

- Wdrożenie ochrony treści serwerów WWW na bazie produktu Cisco Web Content Security

5. Dzień piąty

- Wdrożenie tunelu VPN punkt-punkt typu IOS VTI na bazie routera Cisco
- Wdrożenie tunelu VPN punkt-punkt na bazie Cisco ASA oraz Cisco FirePower
- Wstęp do tuneli VPN typu Remote Access
- Wdrożenie tunelu VPN typu Remote Access na bazie Cisco ASA oraz Cisco FirePower

6. Tematyka uzupełniająca (nauka własna)

- Wstęp do tematyki ochrony informacji
- Charakterystyka działania typowych ataków w sieciach komputerowych w warstwie L3/L4
- Charakterystyka działania typowych ataków w sieciach komputerowych w warstwie aplikacji
- Charakterystyka działania typowych ataków ukierunkowanych na stacje końcowe
- Wdrożenie rozwiązania Cisco Umbrella
- Wyjaśnienie działania typowych mechanizmów kryptograficznych stosowanych w tunelach VPN
- Charakterystyka i konfiguracja protokołu 802.1X
- Charakterystyka rozwiązania Cisco AMP dla urządzeń końcowych

- Wdrożenie mechanizmów ochrony płaszczyzny kontrolnej na urządzeniach L2 i L3
- Ochrona płaszczyzny zarządzania urządzeniami sieciowymi
- Ochrona produktów w chmurze przy użyciu produktu Cisco Stelthwatch
- Opis rozwiązania SDN