Implementing and Operating Cisco Security Core Technologies

Szkolenie autoryzowane Cisco.

Płać punktami CLC:

Cisco Learning Credits accepted : **23 Credits** per Class

Więcej informacji na temat wymagań znajdziesz na stronie:

https://www.altkomakademia.pl/add-content/trainings/cisco-learning-credits.pdf

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 opłata 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.

PRZYGOTOWANIE DO SZKOLENIA

Wirtualna Klasa

- Poznanie trenera i grupy
- Sprawdzanie wiedzy - testy i quizy
- Wprowadzenie w temat zajęć

WYKŁADY I WARSZTATY

Sala szkoleniowa

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

WSPARCIE I ROZWÓJ PO SZKOLENIU

Portal Altkom Akademii

- Dostęp do materiałów szkoleniowych i uzupełniających
- Opieka trenera
- Kontakt ze społecznością

Kod szkolenia	SCOR / PL AA 5d
Czas trwania	5 dni
Poziom	Średnio zaawansowany
Autoryzacja	CISCO