kod szkolenia: SCOR / PL DL 5d

Implementing and Operating Cisco Security Core Technologies v 2.0

Szkolenie autoryzowane Cisco.

Szkolenie "Implementing and Operating Cisco Security Core Technologies (SCOR)" pomaga zdobyć umiejętności oraz technologie niezbędne do wdrożenia kluczowych rozwiązań zabezpieczających Cisco. Szkolenie to przygotuje Cię do zapewnienia zaawansowanej ochrony przed cyberatakami oraz do objęcia stanowisk na wyższym szczeblu w dziedzinie bezpieczeństwa.

Kurs przygotowuje do egzaminu 350-701 SCOR v1.1. Po jego zdaniu uzyskuje się certyfikat Cisco Certified Specialist - Security Core, który spełnia wymagania egzaminu podstawowego dla certyfikatów Cisco Certified Network Professional (CCNP) Security oraz Cisco Certified Internetwork Expert (CCIE) Security.

Płać punktami CLC:

Cisco Learning Credits accepted : 43 Credits

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

Odbiorcy szkolenia

- Inżynierowie ds. bezpieczeństwa
- Inżynierowie sieci
- Projektanci sieci
- Administratorzy sieci
- Inżynierowie systemowi
- Konsultanci ds. inżynierii systemów
- Architekci rozwiązań technicznych
- Integratorzy Cisco oraz partnerzy
- Menedżerowie sieci
- Menedżerowie programów
- Kierownicy projektów

Korzyści

- 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.
- Ćwiczenia do samodzielnej realizacji pozwolą na utrwalenie zdobytej wiedzy.
- Przygotujesz się do egzaminu 350-701 SCOR v1.1.
- Uzyskasz 64 punkty z zakresu ciągłej edukacji (CE) niezbędne do recertyfikacji.

Program szkolenia

1. Technologie zabezpieczeń sieciowych
2. Wdrożenie Cisco Secure Firewall ASA

3. Podstawy Cisco Secure Firewall Threat Defense
4. Cisco Secure Firewall Threat Defense – polityki IPS, antymalware i zarządzania plikami
5. Podstawy Cisco Secure Email Gateway
6. Konfiguracja polityk Cisco Secure Email
7. Wdrożenie Cisco Secure Web Appliance
8. Technologie VPN i koncepcje kryptografii
9. Rozwiązania Cisco Secure Site-to-Site VPN
10. Punkt-punktowe VPN IPsec oparte na VTI w Cisco IOS
11. Punkt-punktowe VPN IPsec na Cisco Secure Firewall ASA oraz Cisco Secure Firewall Threat Defense
12. Rozwiązania Cisco Secure Remote-Access VPN
13. Zdalne SSL VPN na Cisco Secure Firewall ASA oraz Cisco Secure Firewall Threat Defense
14. Koncepcja bezpieczeństwa informacji
15. Opis typowych ataków TCP/IP
16. Opis typowych ataków na aplikacje sieciowe
17. Typowe ataki na punkty końcowe
18. Wdrożenie Cisco Umbrella
19. Technologie zabezpieczenia punktów końcowych
20. Cisco Secure Endpoint
21. Rozwiązania Cisco Secure Network Access
22. Uwierzytelnianie 802.1X
23. Konfiguracja uwierzytelniania 802.1X
24. Ochrona infrastruktury sieciowej
25. Bezpieczeństwo płaszczyzny kontrolnej
26. Mechanizmy ochrony płaszczyzny danych (warstwa 2)
27. Mechanizmy ochrony płaszczyzny danych (warstwa 3)
28. Rozwiązania zabezpieczające płaszczyznę zarządzania
29. Metody telemetrii ruchu sieciowego
30. Wdrożenie Cisco Secure Network Analytics
31. Chmura obliczeniowa i bezpieczeństwo chmury
32. Bezpieczeństwo chmury
33. Wdrożenie Cisco Secure Cloud Analytics
34. Sieci definiowane programowo

Oczekiwane przygotowanie uczestnika

Nie ma wymagań wstępnych do tego szkolenia. Niemniej jednak zaleca się posiadanie następującej wiedzy i umiejętności przed jego rozpoczęciem:

- Znajomość sieci Ethernet i TCP/IP
- Praktyczna znajomość systemu operacyjnego Windows

- Praktyczna znajomość sieci i koncepcji Cisco IOS
- Podstawowa znajomość koncepcji zabezpieczeń sieciowych

Umiejętności te można zdobyć dzięki ofercie szkoleniowej Cisco: Implementing and Administering Cisco Solutions (CCNA®).

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

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

Czas trwania

5 dni / 35 godzin

Opis egzaminu

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