kod szkolenia: SWSA / PL AA 2d

Securing the Web with Cisco Web Security Appliance v3.0

Szkolenie autoryzowane Cisco.

Płać punktami CLC:

Cisco Learning Credits accepted : 20 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.

SWSA: 16 punktów CE

Przeznaczenie szkolenia

Szkolenie dla osób planujących przeprowadzenie skutecznego procesu instalacji i późniejszej administracji oraz rozwiązywania problemów z urządzeniami Cisco Web Security Appliance.

Korzyści wynikające z ukończenia szkolenia

Kurs SWSA pomaga przygotować się do certyfikacji Cisco® CCNP® Security i CCIE® Security oraz do pracy na stanowisku starszego inżyniera bezpieczeństwa teleinformatycznego. Na tym kursie opanujesz umiejętności i technologie potrzebne do wdrożenia produktu Cisco WSA. Dowiesz się w jaki sposób chronić sieć przed atakami ukierunkowanymi na serwery WWW. Będziesz umiał monitorować oraz rozwiązywać problemy z działaniem Cisco WSA.

Opis egzaminu

Szkolenie przygotowuje do egzaminu 300-725 SWSA, 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

Dobra znajomość podstaw TCP/IP, adresacji IP, routingu, DNS, SSH, FTP, HTTP(s) oraz protokołu TCP
Wiedza na poziomie szkolenia CCNA oraz SCOR

Jako uzupełnienie rekomendujemy:
Kursy ze ścieżki CCNP Security, które są kontynuacją omawianych zagadnień:

1. Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)
2. Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)
3. Implementing and Configuring Cisco Identity Services Engine (SISE)
4. Securing Email with Cisco Email Security Appliance (SESA)
5. Implementing Secure Solutions with Virtual Private Networks (SVPN)
6. Implementing Automation for Cisco Security Solutions (SAUI)

Język szkolenia

Szkolenie: polski
Materiały: angielski

Czas trwania

2 dni / 14 godzin

Agenda szkolenia

1. **Dzień pierwszy**
   1. Charakterystyka produktu Cisco WSA
      - Przegląd rozwiązania Cisco WSA
      - Przegląd produktów Cisco WSA
      - Architektura wdrożenia protokołu WSA
      - Funkcjonalność serwera proxy
      - Zintegrowany filtr ruchu warstwy 4 ISO/OSI
      - Mechanizm DLP
      - Narzędzia do zarządzania WSA
      - Cisco ASWR
      - Analiza treści SMA
   2. Wdrożenie usługi serwera proxy
      - Tryb transparenty oraz bezpośredniego przekazywania ruchu
      - Przekierowanie ruchu w trybie transparentnym
      - Protokół WCCP
      - Przepływ ruchu do i z serwera WWW w kontekście protokołu WCCP
      - Wyjątki filtrowania przez serwer proxy
      - Przechowywanie treści w pamięci podręcznej cache
      - Pliki typu PAC
      - Usługa proxy dla protokołu FTP oraz SOCKS
      - Podgląd dziennika zdarzeń proxy oraz nagłówków HTTP
      - Dostrajanie komunikatów o błędach
   3. Obsługa mechanizmu uwierzytelniania
      - Protokoły służące do uwierzytelniania
      - Śledzenie danych uwierzytelniających użytkowników
      - Omijanie weryfikacji danych uwierzytelniających
      - Raportowanie zdarzeń związanych z uwierzytelnianiem
      - Mechanizmy proxy dla uwierzytelniania z użyciem FTP
      - Rozwiązywanie problemów z dołączaniem WSA do AD
      - Integracja WSA z Cisco ISE

4. Tworzenie zasad deszyfracji ruchu celem inspekcji ruchu HTTPS
    - Charakterystyka inspekcji ruchu zaszyfrowanego przy użyciu TLS/SSL
    - Certyfikaty cyfrowe
    - Charakterystyka zasad deszyfracji ruchu HTTPS
    - Aktywacja funkcjonalności proxy HTTPS
    - Znakowanie ruchu, który ma być poddany inspekcji przy użyciu ACL
5. Tworzenie zasad obsługi klas ruchu sieciowego
    - Przegląd mechanizmów kontroli dostępu
    - Grupowanie zasad kontroli dostępu
    - Charakterystyka profilu klasy ruchu sieciowego
    - Kolejność przetwarzania zasad kontroli dostępu oraz profili klas ruchu sieciowego
    - Inne typy reguł dostępu
    - Przykłady zawartości dziennika zdarzeń
    - Znaczniki ACL
    - Stosowanie zasad czasowych oraz odnoszących się do ilości ruchu użytkownika

2. **Dzień drugi**

6. Ochrona przed złośliwym oprogramowaniem
    - Filtry bazujące na reputacji
    - Skanowanie pod kątem złośliwego oprogramowania
    - Skanowanie ruchu wychodzącego
    - Zasady kontroli filtrujące przychodzący ruch pod kątem złośliwego oprogramowania
    - Filtrowanie plików na bazie reputacji oraz dogłębnej analizy
    - Integracja WSA z bazami danych Cisco Intelligence
7. Kontrola dostępu ustawień użytkownika
    - Kontrolowanie korzystania z sieci Internet
    - Filtrowanie URL
    - Kategorie URL
    - Mechanizm dynamicznej kontroli treści
    - Wykrywanie aplikacji z których korzystają użytkownicy
    - Limity przepustowości
    - Filtrowanie treści dla osób pełnoletnich
8. Ochrona danych przy użyciu mechanizmu DLP
    - Ochrona danych
    - Rozwiązanie Cisco do ochrony danych
    - Definicja zasad ochrony danych
    - Dziennik zdarzeń mechanizmu DLP
9. Czynności administracyjne oraz rozwiązywanie problemów z WSA
    - Monitorowanie działania WSA
    - Raporty generowane z WSA
    - Monitorowanie działania rozwiązana z użyciem dzienników zdarzeń

- Czynności administracyjne
- Rozwiązywanie problemów z WSA
- CLI WSA