Możliwość dofinansowania

Dagma sp. z o.o.

Certified Stormshield Network Administrator (CSNA)

Numer usługi 2024/11/21/17164/2424371

4 292,70 PLN brutto
3 490,00 PLN netto
178,86 PLN brutto/h
145,42 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
26.11.2024 do 28.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane zarówno dla osób, które właśnie nabyły urządzenie Stormshield oraz dla tych, którzy w praktyczny sposób chcą zapoznać się z możliwościami rozwiązania. Uczestnicy szkolenia powinny spełniać poniższe wymagania: • podstawowa znajomość konfiguracji sieci komputerowych; • podstawowa znajomość zagadnień związanych z TCP/IP.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	23-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie kompetencji z zakresu produktu Certified Stormshield Network Administrator (CSNA), dzięki którym uczestnik samodzielnie dokona audytów bezpieczeństwa sieci, szybko zdiagnozuje i usunie problemy w sieci oraz umiejętnie rozstrzygnie dylematy związane z codzienną pracą w dziale IT. Dzięki szkoleniu uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie oraz rozwiązywanie problemów.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zarządza urządzeniami Stormshield; kontroluje dostępami do stron internetowych (http i https); wdraża urządzenia Stormshield w sieci firmowej, definiuje polityki filtrowania (Firewall i NAT) oraz trasy routingu, konfiguruje polityki bezpieczeństwa dla uwierzytelnionych użytkowników, wdraża różne typy wirtualnych sieci prywatnych (VPN) - IPSec VPN i SSL VPN.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, dokument stanowi potwierdzenie, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument potwierdza, że zostały zastosowane rozwiązania zapewniające rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

MODUŁ 1 Rozpoczęcie pracy z urządzeniem - zajęcia teoretyczne (wykład)

- Rejestracja w strefie klienta i dostęp zasobów
- Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
- Ustawienia systemowe i uprawnienia administratorów
- Instalacja licencji i aktualizacja systemu

- Tworzenie kopii zapasowej i przywracanie konfiguracji

MODUŁ 2 Zbieranie logów i monitorowanie - zajęcia teoretyczne (wykład)

- Przedstawienie kategorii zbieranych logów
- Wykresy historyczne i monitorowanie

Obiekty

- Typy obiektów oraz ich wykorzystanie
- Obiekty sieciowe i obiekt typu „router”

MODUŁ 3 Konfiguracja sieci - zajęcia praktyczne (ćwiczenia)

- Tryby pracy urządzenia
- Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
- Typy routingu oraz ich priorytety

MODUŁ 4 Translacja adresów sieciowych (NAT) - zajęcia praktyczne (ćwiczenia)

- Translacja połączeń wychodzących (maskarada)
- Translacja połączeń przychodzących (przekierowanie)
- Translacja dwukierunkowa (jeden do jeden)

MODUŁ 5 Filtrowanie ruchu sieciowego (Firewall) - zajęcia praktyczne (ćwiczenia)

Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)

- Szczegółowy opis parametrów reguły Firewall
- Kolejność przetwarzania reguł Firewall i NAT

MODUŁ 6 Ochrona aplikacji - zajęcia praktyczne (ćwiczenia)

- Implementacja filtrowania URL dla ruchu http i https
- Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
- Moduł IPS i stosowanie profili inspekcji

MODUŁ 7 Użytkownicy i uwierzytelnianie - zajęcia teoretyczne (wykład)

1. Konfiguracja usługi katalogowej
   - Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
   - Rejestracja użytkowników
   - Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania

MODUŁ 8 Wirtualne sieci prywatne (VPN) - zajęcia praktyczne (ćwiczenia)

- Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
- Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
- Tunele VTI

MODUŁ 9 SSL VPN - zajęcia teoretyczne (wykład)

- Zasada działania
- Konfiguracja
- **Walidacja**

Szkolenie składa się z 10 godzin teoretycznych (w postaci wykładu) oraz 11 godzin praktycznych (w postaci ćwiczeń), w tym:

- Moduł 1: dwie godziny teoretyczne (2x 45 minut)
- Moduł 2: trzy godziny teoretyczne (3x 45 minut)
- Moduł 3: pięć godzin praktycznych (3x 45 minut)
- Moduł 4: dwie godziny praktyczne (2x 45 minut)
- Moduł 5: trzy godziny praktyczne (3x 45 minut)
- Moduł 6: trzy godziny praktyczne (3x 45 minut)
- Moduł 7: dwie godziny teoretyczne (2x 45 minut)
- Moduł 8: trzy godziny praktyczne (3x 45 minut)
- Moduł 9: trzy godziny teoretyczne z walidacją (3x45 minut)

Razem 21 godzin lekcyjnych, (18 zegarowych):

- walidacja jest wliczona w czas szkolenia
- przerwy

  nie są

  wliczone w czas trwania szkolenia.

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 MODUŁ 1 Rozpoczęcie pracy z urządzeniem - zajęcia teoretyczne (wykład)	Adam Ferenc	26-11-2024	09:00	10:30	01:30
2 z 10 MODUŁ 2 Zbieranie logów i monitorowanie - zajęcia teoretyczne (wykład)	Adam Ferenc	26-11-2024	10:45	13:00	02:15
3 z 10 MODUŁ 3 Konfiguracja sieci - zajęcia praktyczne (ćwiczenia)	Adam Ferenc	26-11-2024	13:30	15:45	02:15
4 z 10 MODUŁ 4 Translacja adresów sieciowych (NAT) - zajęcia praktyczne (ćwiczenia)	Adam Ferenc	27-11-2024	09:00	10:30	01:30
5 z 10 MODUŁ 5 Filtrowanie ruchu sieciowego (Firewall) - zajęcia praktyczne (ćwiczenia)	Adam Ferenc	27-11-2024	10:45	13:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 10 MODUŁ 6 Ochrona aplikacji - zajęcia praktyczne (ćwiczenia)	Adam Ferenc	27-11-2024	13:30	15:45	02:15
7 z 10 MODUŁ 7 Użytkownicy i uwierzytelnianie - zajęcia teoretyczne (wykład)	Adam Ferenc	28-11-2024	09:00	10:30	01:30
8 z 10 MODUŁ 8 Wirtualne sieci prywatne (VPN) - zajęcia praktyczne (ćwiczenia)	Adam Ferenc	28-11-2024	10:45	13:00	02:15
9 z 10 MODUŁ 9 SSL VPN - zajęcia teoretyczne (wykład)	Adam Ferenc	28-11-2024	13:30	15:25	01:55
10 z 10 Walidacja	-	28-11-2024	15:25	15:45	00:20

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 292,70 PLN
Koszt przypadający na 1 uczestnika netto	3 490,00 PLN
Koszt osobogodziny brutto	178,86 PLN
Koszt osobogodziny netto	145,42 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adam Ferenc

Doświadczenie zawodowe: Trener IT w DAGMA Szkolenia IT od 2016 roku, specjalista w zakresie produktów cyberbezpieczeństwa firmy STORMSHIELD. Prowadzący szkolenia, wdrożenia, konsultacje związane z produktami UTM.
Specjalizacja: zagadnienia sieciowe, bezpieczeństwo na poziomie rozwiązań ESET, Stormshield. VPN
Certyfikaty: Certyfikat trenerski Stormshield Network Administrator
Wykształcenie: wyższe, licencjackie, Ekspertyza cybernetyczna/komputerowa i przeciwterrorystyczna

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-podręcznik i/lub materiały autorskie, przygotowane przez producenta rozwiązań Stormshield)
- dostęp do przygotowanego środowiska wirtualnego na platformie Stormshield na czas trwania szkolenia

Warunki uczestnictwa

Wymagania sprzętowe:

- System operacyjny: Windows 64-bit,
- Karta sieciowa Ethernet,
- Użytkownik musi mieć także pełne prawa administracyjne celem skonfigurowania połączeń sieciowych oraz instalacji oprogramowania (SSL VPN client),
- Wymagana jest także aktualna przeglądarka WWW (Mozilla Firefox/ Microsoft Edge/ Google Chrome).

Informacje dodatkowe

- Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl**

Informacje organizacyjne:

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.

- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia

- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA Szkolenia IT.

Warunki techniczne

WARUNKITECHNICZNE:

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) do udziału w szkoleniu potrzebne będzie:

- łącze internetowe o przepustowości minimum 10Mbit,
- dostęp do Internetu na portach 1194/UDP i 443/TCP,
- komputer z 64-bitowym systemem operacyjnym Microsoft Windows z klientem pulpitu zdalnego,
- zainstalowane w systemie operacyjnym oprogramowanie Stormshield SSL VPN Client. Oprogramowanie można pobrać z tego adresu: http://data.stormshield.eu/data2/sns/VPNSSL/2.8.0/signed-Stormshield_SSLVPN_Client_2.8.0_en_x64.msi

UWAGA: Jeżeli w systemie operacyjnym jest zainstalowane oprogramowanie OpenVPN to przed instalacją klienta Stormshield SSL VPN należy je odinstalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl
Telefon (+48) 32 7931 139