



Dagma sp. z o.o.

**Certified Stormshield Network
Troubleshooting & Support (NT-CSNTS)**

Numer usługi 2024/07/02/17164/2206290

zdalna w czasie rzeczywistym

Usługa szkoleniowa

30 h

05.08.2024 do 09.08.2024

12 177,00 PLN brutto

9 900,00 PLN netto

405,90 PLN brutto/h

330,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	<p>Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania:</p> <ul style="list-style-type: none">• znajomość języka angielskiego na poziomie B2 (szkolenie prowadzone w języku angielskim)• zaawansowana znajomość TCP/IP i UNIX,• ważny certyfikat CSNE (Certified Stormshield Network Expert).
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	29-07-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	30
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

Celem szkolenia jest dostarczenie kompetencji z zakresu Certified Stormshield Network Troubleshooting & Support (NT-CSNTS), dzięki którym uczestnik będzie samodzielnie analizował polityki bezpieczeństwa i identyfikował jej ogólne wytyczne i parametry specjalne, analizował i debugował konfiguracje wysokiej dostępności. Uczestnik po ukończonym szkoleniu nabędzie kompetencje społeczne takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wie, jak przebiega: organizacja systemu plików i procesów w Stormshield, identyfikacja procesów stosowanych do trwających połączeń, analiza i debugowanie konfiguracji wysokiej dostępności, analiza polityki bezpieczeństwa i identyfikacja jej ogólne wytycznych i parametrów specjalnych.	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik nabędzie umiejętność lokalizacji, eksploracji i obsługi różnych plików konfiguracyjnych oraz dzienników; przechwytywania i analizy ruchu sieciowego; generowania dostosowanego, kompleksowego i użytecznego raportu; skonfigurowania polityki tuneli IPSec VPN, identyfikacja włączonych mechanizmów i diagnozowanie awarii tych mechanizmów	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak

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

Tak

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

tAK

Program

Moduł 1: Funkcjonalności SSH - zajęcia teoretyczne (wykład)

- System plików i związane z nim polecenia
- Katalogi i związane z nimi polecenia
- System i środowisko użytkownika
- Pliki i związane z nimi polecenia

Moduł 2: Logi - zajęcia praktyczne (ćwiczenia)

- Logi lokalne: lokalizacja, charakterystyka, składnia i kategorie
- Powiązane polecenia
- Pliki konfiguracyjne
- Logd, logctl, logi komunikatów jądra

Moduł 3: Pliki konfiguracyjne - zajęcia praktyczne (ćwiczenia)

- Katalogi, struktura i ogólna składnia
- Kopie zapasowe (*.na), debackup i tar
- Konfiguracja domyślna

Moduł 4: Obiekty - zajęcia teoretyczne (wykład)

- Składnia obiektu
- Obiekty dynamiczne i FQDN

Moduł 5: Sieć i routing - zajęcia teoretyczne (wykład)

- Ustawienia interfejsu sieciowego
- Urządzenia sieciowe typy most i związane z nimi polecenia
- Funkcje routingu i ich priorytety
- Trasy domyślne i trasy statyczne
- Obiekty bramek i routerów
- Routing dynamiczny
- polecenia względne i pokazywanie tras
- Tryb szczegółowy

Laboratorium: Sieć i routing

Moduł 6: Przechwytywanie i analiza ruchu - zajęcia praktyczne (ćwiczenia)

- Wprowadzenie i wskazówki
- Ogólna składnia i argumenty
- Filtry wspólne
- Skomentowane przykłady i przygotowania do skutecznych chwytów
- Analiza ruchu za pomocą tcpdump (ruch TCP i UDP/icmp)

Laboratorium: Sieć/tcpdump

Moduł 7: ASQ: różne etapy jego analizy - zajęcia teoretyczne (wykład)

- Analiza krok po kroku warstw sieci
- Powiązane polecenia
- Ustawienia globalne
- Specjalne profile i ustawienia
- Asynchroniczne ASQ: różne przypadki i znaki wodne
- Tryb gadatliwy ASQ

Laboratorium: ustawienia ASQ

Moduł 8: ASQ: polityka bezpieczeństwa - zajęcia praktyczne (ćwiczenia)

- Pliki i katalogi konfiguracyjne oraz składnia reguł
- Filtrowanie: powiązane polecenia
- Filtrowanie: przykłady załadowanych reguł (akcja, poziom kontroli, wtyczka, PBR, QoS, interfejsy i proxy)
- Filtrowanie: tłumaczenie grup i list
- NAT: wersja (dynamiczny NAT, statyczny NAT według portu, statyczny NAT/bimap i nie NAT)
- NAT: powiązane polecenia
- NAT: składnia załadowanych reguł

Laboratorium: NAT i filtrowanie

Moduł 9 ASQ: śledzenie stanów i tabele stanu - zajęcia teoretyczne (wykład)

- Chroniona tablica adresów
- Stół hosta
- Tabela połączeń: przykłady stanów połączeń (NAT, vconn, wtyczka FTP, asynchroniczna, lite itp.)

Laboratorium: śledzenie stanowe ASQ

Moduł 10: Procesy typu daemon - zajęcia praktyczne (ćwiczenia)

- Listy i role
- Procesy typu supervisor daemon
- Polecenia względne
- Eventd: event manager

Moduł 11: IPSec VPN - zajęcia teoretyczne (wykład)

- Wdrożenie IKE/IPsec sieci Stormshield
- Pliki konfiguracyjne
- Polityka bezpieczeństwa (SPD i SAD)
- Negocjacje IKE
- Negocjacje: tryb główny i tryb agresywny
- ISAKMP i IPsec SA
- Propozycje IKE
- Specyficzne cechy: NAT-T, DPD, Keepalive, SharedSA, Policy None i SPD

Moduł 12: Cache - zajęcia praktyczne (ćwiczenia)

- Powiązane polecenia
- Analiza IPsec-SA
- Dzienniki
- Powiadomienia „Delete SA”
- ISAKMP przechwytuje i analizuje ruch
- Specyfika dynamicznych rówieśników
- Tryb szczegółowy i typowe błędy

Laboratorium: ISAKMP/IPsec

Moduł 13: PKI i certyfikaty- zajęcia teoretyczne (wykład)

- Podsumowanie i dyrektywy globalne
- Katalog CA
- Wskazówki dotyczące konfiguracji
- Weryfikacja certyfikatu

Moduł 14: Duża dostępność - zajęcia praktyczne (ćwiczenia)

- Przegląd
- Pliki konfiguracyjne
- Polecenia względne
- Włączanie HA i zarządzanie interfejsami sieciowymi
- Zaangażowane procesy i ruch
- Replikacje/synchronizacja

- Zdarzenia i dzienniki HA

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 30godz. lekcyjnych). Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	12 177,00 PLN
Koszt przypadający na 1 uczestnika netto	9 900,00 PLN
Koszt osobogodziny brutto	405,90 PLN
Koszt osobogodziny netto	330,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-book, lub dostęp do materiałów autorskich, przygotowanych przez trenera, przesłane na adres e-mail uczestnika)
- dostęp do przygotowanego środowiska wirtualnego

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową www.acsdagma.com.pl w celu rezerwacji miejsca.

Informacje dodatkowe

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzi koszt związany z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Uczestnik otrzymuje zaświadczenie ACS 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 Autoryzowane Centrum Szkoleniowe DAGMA.

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.

Oprogramowanie Stormshield SSL VPN Client należy zainstalować przed rozpoczęciem szkolenia (najlepiej 1 dzień przed szkoleniem). W razie jakichkolwiek problemów technicznych z jego instalacją prosimy o kontakt na adres: [**szkolenia@dagma.pl**](mailto:szkolenia@dagma.pl)

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi (czyt. od 5 września do 9 września)

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl



Telefon (+48) 322 591 139