



Dagma sp. z o.o.

**CERTIFIED STORMSHIELD NETWORK
EXPERT (CSNE)**

Numer usługi 2025/05/19/17164/2755091

zdalna w czasie rzeczywistym

Usługa szkoleniowa

24 h

24.06.2025 do 26.06.2025

4 538,70 PLN brutto

3 690,00 PLN netto

189,11 PLN brutto/h

153,75 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: posiadanie certyfikatu Certified Stormshield Network Administrator (CSNA)
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	16-06-2025
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

Celem szkolenia jest dostarczenie kompetencji z zakresu działania programu STORMSHIELD NETWORK EXPERT, dzięki którym uczestnik będzie samodzielnie konfigurował i implementował rozwiązania UTM, konfigurował serwer IPSEC,

VPN, a także konfigurował urządzenia z poziomu CL. 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
Skonfigurować zaawansowane funkcje bezpieczeństwa urządzeń Stormshield z poziomu GUI i CLI – efektywnie wykorzystuje interfejsy konfiguracyjne do zarządzania urządzeniem oraz implementacji zaawansowanych polityk bezpieczeństwa. Zarządzać i konfigurować silnik IPS – dostosowuje profile IPS na podstawie protokołów i aplikacji, rozróżnia tryby pracy IPS/IDS i konfiguruje odpowiednie reguły ochrony. Projektować i wdrażać tunele VPN z wykorzystaniem technologii IPSec, GRE i GREtAP – konfiguruje tunelowanie Site-to-Site i Client-to-Site z uwzględnieniem mechanizmów NAT traversal, DPD i redundantnych połączeń.	Ćwiczenie: Konfiguracja silnika IPS z wykorzystaniem trybów i profili – uczestnik konfiguruje silnik IPS dla wybranych protokołów i aplikacji, testuje skuteczność reguł oraz interpretuje logi. Zadanie: Konfiguracja tunelu IPSec VPN typu Site-to-Site z użyciem certyfikatów – uczestnik tworzy i testuje tunel VPN, uwzględniając redundancję i NAT traversal. Ćwiczenie praktyczne: Instalacja i konfiguracja GRE oraz GREtAP – uczestnik poprawnie konfiguruje oba typy tunelowania oraz weryfikuje poprawność przesyłania danych.	Obserwacja w warunkach symulowanych
Zarządzać infrastrukturą klucza publicznego (PKI) i certyfikatami w środowisku Stormshield – tworzy urzędy certyfikacji, generuje i stosuje certyfikaty serwera i użytkowników, stosuje SSL Proxy i certyfikaty do uwierzytelniania. Zaimplementować transparentne uwierzytelnianie użytkowników – konfiguruje metody SPNEGO oraz certyfikaty SSL do automatycznej identyfikacji użytkowników w sieci. Zarządzać konfiguracją urządzeń Stormshield w trybie wysokiej dostępności (HA) – konfiguruje klastry HA, interfejsy sieciowe i nadzoruje poprawność pracy w środowiskach redundantnych. Analizować ruch sieciowy oraz diagnozować i rozwiązywać problemy konfiguracyjne – wykorzystuje wbudowane narzędzia i raporty urządzeń do bieżącej analizy aktywności i logów systemowych.	Symulacja: Konfiguracja infrastruktury PKI i zastosowanie SSL Proxy – uczestnik tworzy CA, wystawia certyfikaty, konfiguruje SSL Proxy i weryfikuje skuteczność deszyfrowania. Zadanie: Uwierzytelnianie użytkowników z użyciem SPNEGO i certyfikatów SSL – uczestnik konfiguruje mechanizm transparentnego uwierzytelniania i testuje jego działanie. Test: Konfiguracja klastra HA i analiza działania po awarii – uczestnik konfiguruje HA i przeprowadza symulację awarii w celu weryfikacji przełączania.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji	Wywiad swobodny

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 Szczegółowe omówienie działania modułu IPS od Stormshield - zajęcia teoretyczne (wykład)

- Różnice pomiędzy IPS a IDS
- moduł IPS
- Różne tryby analizy
- Profile oparte na protokołach i aplikacjach

Moduł 2 Infrastruktura klucza publicznego - zajęcia teoretyczne (wykład)

- Podstawy szyfrowania symetrycznego - i asymetrycznego
- Typy szyfrowania
- Infrastruktura klucza publicznego - w rozwiązaniach Stormshield
- Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników

Moduł 3 SSL Proxy - zajęcia praktyczne (ćwiczenia)

- Zasada działania
- Konfiguracja SSL Proxy
- Zaawansowana konfiguracja tuneli IPSec VPN
- Szczegółowy opis działania mechanizmu NAT traversal
- Obsługa funkcji DPD (Dead Peer Detection)
- Architektura sieci VPN typu „gwiazda” i „mesh”

- NAT w sieciach IPSec VPN
- Konfiguracja zapasowego - tunelu IPSec VPN
- Konfiguracja tuneli Site-to-Site w oparciu - certyfikaty
- Konfiguracja tuneli dla użytkowników mobilnych (Client-2-Site)

Moduł 4 GRE i GRE-TAP - zajęcia praktyczne (ćwiczenia)

- Zasada działania
- Konfiguracja i instalacja

Moduł 5 Transparentne uwierzytelnianie użytkowników - zajęcia teoretyczne (wykład)

- Zasada działania
- Metoda uwierzytelniania SPNEGO
- Metoda uwierzytelniania oparta na certyfikatach SSL

Moduł 6 Wysoka dostępność (HA) - zajęcia praktyczne (ćwiczenia)

- Zasada działania
- Kreator umożliwiający tworzenie i konfigurowanie klastra HA
- Konfiguracja interfejsu sieciowego
- Zaawansowana konfiguracja

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 24 godz. 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	4 538,70 PLN
Koszt przypadający na 1 uczestnika netto	3 690,00 PLN
Koszt osobogodziny brutto	189,11 PLN
Koszt osobogodziny netto	153,75 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Adam Ferenc

Trener IT w ACS Dagma od 2016 roku, prowadzący szkolenia z zakresu produktów Stormshield od 2018r. Obszar specjalizacji:

zagadnienia sieciowe, bezpieczeństwo na poziomie rozwiązań ESET, Stormshield.

Doświadczenia zawodowe:

2013 – do teraz – wsparcie techniczne rozwiązań ESET, Stormshield, Deslock, StorageCraft, Barracuda.

Doświadczenia w świadczeniu tego typu usług:

Wdrożenia ESET, Stormshield (w tym u klientów 1000+).

Szkolenia ESET, Stormshield, bezpieczeństwo użytkownika końcowego.

Wykształcenie: Wyższe informatyczne. Zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-podręcznik i/lub dostęp do materiałów autorskich, przygotowanych przez trenera Stormshield) przesyłany na adres mailowy uczestnika;
- dostęp do przygotowanego środowiska wirtualnego na platformie Stormshield

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową <https://szkolenia.dagma.eu/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 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 Autoryzowane 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.

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***

e) okres ważności linku:

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

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie:

<https://www.acsdagma.com/pl/szkolenia-online>

Kontakt



Agnieszka Palenga

E-mail palenga.a@dagma.pl

Telefon (+48) 32 7931 139