



## Certified Stormshield Network Administrator (CSNA)

Numer usługi 2024/07/02/17164/2206314

4 292,70 PLN brutto

3 490,00 PLN netto

178,86 PLN brutto/h

145,42 PLN netto/h

Dagma sp. z o.o.



📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 24 h

📅 06.08.2024 do 08.08.2024

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
<b>Grupa docelowa usługi</b>	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: <ul style="list-style-type: none"><li>• podstawowa znajomość konfiguracji sieci komputerowych;</li><li>• podstawowa znajomość zagadnień związanych z TCP/IP.</li></ul>
<b>Minimalna liczba uczestników</b>	5
<b>Maksymalna liczba uczestników</b>	8
<b>Data zakończenia rekrutacji</b>	30-07-2024
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	24
<b>Podstawa uzyskania wpisu do BUR</b>	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 wie, jak sprawnie zarządzać urządzeniami Stormshield; Uczestnik nabędzie umiejętności: kontrolowania dostępu do stron internetowych (http i https); Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	Samodzielna praca w środowisku wirtualnym	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 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, GRE/TAP)
- 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

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	4 292,70 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: 0

Brak wyników.

## 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

### 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 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 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 udostępnić 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/VPNSSSL/2.8.0/signed-Stormshield\\_SSLVPN\\_Client\\_2.8.0\\_en\\_x64.msi](http://data.stormshield.eu/data2/sns/VPNSSSL/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