

**Certified Stormshield Network Administrator (CSNA)**

Numer usługi 2026/07/09/17164/3678953

4 415,70 PLN brutto

3 590,00 PLN netto

183,99 PLN brutto/h

149,58 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Dagma sp. z o.o.

★★★★★ 4,5 / 5

469 ocen

🏠 Usługa szkoleniowa

📺 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 24:00 h

📅 27.10.2026 do 29.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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 powinni 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	19-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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; wdraża urządzenia Stormshield w sieci firmowej, definiuje polityki filtrowania (Firewall i NAT) oraz trasy routingu,	kontroluje dostępami do stron internetowych (http i https);	Obserwacja w warunkach symulowanych
konfiguruje polityki bezpieczeństwa dla uwierzytelnionych użytkowników,	wdraża różne typy wirtualnych sieci prywatnych (VPN) - IPSec VPN i SSL VPN.	Obserwacja w warunkach symulowanych
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 lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają 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
- **Walidacja**

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

Harmonogram

Liczba pozycji harmonogramu: 19

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 19 1 Rozpoczęcie pracy z urządzeniem - zajęcia teoretyczne (wykład)	Zajęcia	Piotr Spiecha	27-10-2026	09:00	10:30	01:30
2 z 19 -	Przerwa	-	27-10-2026	10:30	11:00	00:30
3 z 19 2 Zbieranie logów i monitorowanie - zajęcia teoretyczne (wykład)	Zajęcia	Piotr Spiecha	27-10-2026	11:00	13:30	02:30
4 z 19 -	Przerwa	-	27-10-2026	13:30	14:00	00:30
5 z 19 MODUŁ 3 Konfiguracja sieci - zajęcia praktyczne (ćwiczenia)	Zajęcia	Piotr Spiecha	27-10-2026	14:00	17:00	03:00
6 z 19 MODUŁ 4 Translacja adresów sieciowych (NAT) - zajęcia praktyczne (ćwiczenia)	Zajęcia	Piotr Spiecha	28-10-2026	09:00	10:30	01:30
7 z 19 -	Przerwa	-	28-10-2026	10:30	11:00	00:30
8 z 19 MODUŁ 5 Filtrowanie ruchu sieciowego (Firewall) - zajęcia praktyczne (ćwiczenia)	Zajęcia	Piotr Spiecha	28-10-2026	11:00	13:30	02:30
9 z 19 -	Przerwa	-	28-10-2026	13:30	14:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 19 MODUŁ 6 Ochrona aplikacji - zajęcia praktyczne (ćwiczenia)	Zajęcia	Piotr Spiecha	28-10-2026	14:00	15:45	01:45
11 z 19 -	Przerwa	-	28-10-2026	15:45	16:00	00:15
12 z 19 MODUŁ 6 Ochrona aplikacji - zajęcia praktyczne (ćwiczenia) cz.2	Zajęcia	Piotr Spiecha	28-10-2026	16:00	17:00	01:00
13 z 19 MODUŁ 7 Użytkownicy i uwierzytelnianie - zajęcia teoretyczne (wykład)	Zajęcia	Piotr Spiecha	29-10-2026	09:00	10:30	01:30
14 z 19 -	Przerwa	-	29-10-2026	10:30	11:00	00:30
15 z 19 MODUŁ 8 Wirtualne sieci prywatne (VPN) - zajęcia praktyczne (ćwiczenia)	Zajęcia	Piotr Spiecha	29-10-2026	11:00	13:30	02:30
16 z 19 -	Przerwa	-	29-10-2026	13:30	14:00	00:30
17 z 19 MODUŁ 9 SSL VPN - zajęcia teoretyczne (wykład)	Zajęcia	Piotr Spiecha	29-10-2026	14:00	16:00	02:00
18 z 19 -	Przerwa	-	29-10-2026	16:00	16:15	00:15
19 z 19 -	Walidacja	-	29-10-2026	16:15	17:00	00:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	24:00
w tym suma godzin zajęć	19:45
w tym suma godzin walidacji	00:45
w tym suma przerw	03:30
Suma godzin dydaktycznych bez przerw	27:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 415,70 PLN
Koszt przypadający na 1 uczestnika netto	3 590,00 PLN
Koszt osobogodziny brutto	183,99 PLN
Koszt osobogodziny netto	149,58 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	24:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Piotr Spiecha

Obszar specjalizacji: Windows Server, Wirtualizacja Hyper-V i VMware oraz chmury Azure

Doświadczenie zawodowe: Wieloletnie doświadczenie w projektowaniu i wdrażaniu systemów teleinformatycznych oraz w prowadzeniu szkoleń, w tym autoryzowanych szkoleń Microsoft. Brał udział wielu projektach wdrożeniowych z zakresu wirtualizacji Microsoft i VMware

Doświadczenie w świadczeniu tego typu usług: Posiada kilkuletnie doświadczenie jako trener ACS Dagma, od 2017 roku prowadzi autoryzowane szkolenia Microsoft

Certyfikaty Microsoft i VMware: MCT - Microsoft Certified Trainer, MCSE, MCSA, MCITP, Azure Expert, Azure Admin, VCP6.5-DCV, VCP5.5-DCV

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 materiały autorskie, przygotowane przez producenta rozwiązań Stormshield)
- dostęp do przygotowanego środowiska wirtualnego na platformie Stormshield na czas trwania szkolenia

Warunki uczestnictwa

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

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

- W cenę szkolenia nie wchodzi koszty związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Harmonogram ma charakter ramowy i trener może na potrzeby grupy szkoleniowej zmienić długość poszczególnych modułów, przy zachowaniu niezmięnionej łącznej liczby godzin usługi szkoleniowej.
- 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.
- Organizator szkolenia zastrzega sobie prawo do zmiany trenera prowadzącego/walidującego jeśli z przyczyn niezależnych od Organizatora (np. zdarzenie losowe) wyznaczony trener nie będzie mógł przeprowadzić szkolenia. Przy czym Organizator zobowiązuje się do zapewnienia w zastępstwie trenera o takich samych/zbliżonych kompetencjach.

Warunki techniczne

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/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



Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 32 7931 180