



Dagma sp. z o.o.

★★★★★ 4,5 / 5

467 ocen

ESET - Protect Expert

Numer usługi 2026/06/25/17164/3650078

📁 Usługa szkoleniowa

📺 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 07:00 h

📅 06.11.2026 do 06.11.2026

2 447,70 PLN brutto

1 990,00 PLN netto

349,67 PLN brutto/h

284,29 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie jest przeznaczone dla:

- **Administratorów IT i specjalistów technicznych**, którzy zarządzają systemami ESET PROTECT w firmie.
- **Osób odpowiedzialnych za wdrożenia i utrzymanie ochrony stacji roboczych i serwerów.**
- **IT-owców chcących pogłębić wiedzę w zaawansowanym zarządzaniu ESET**, w tym konfiguracji polityk bezpieczeństwa i uwierzytelniania.
- **Osób przygotowujących się do certyfikacji producenta** lub chcących rozwijać kompetencje w zakresie bezpieczeństwa IT.

Wymagania wstępne: podstawowa znajomość systemów operacyjnych, sieci i wcześniejsze doświadczenie z ESET PROTECT.

Szkolenie i materiały w języku polskim.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

28-10-2026

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

Celem szkolenia jest nabycie zaawansowanych umiejętności w zarządzaniu i konfiguracji systemu ESET PROTECT, pozwalających na skuteczne wdrażanie, monitorowanie i utrzymanie ochrony stacji roboczych oraz serwerów w środowiskach firmowych, a także rozwiązywanie złożonych problemów bezpieczeństwa IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi zainstalować i skonfigurować agentów ESET PROTECT na różnych systemach operacyjnych.	Poprawna instalacja i rejestracja agentów w konsoli ESET PROTECT.	Obserwacja w warunkach rzeczywistych
Uczestnik umie tworzyć i zarządzać politykami bezpieczeństwa w ESET PROTECT.	Utworzenie polityki działającej zgodnie z założeniami (np. blokada nieautoryzowanego oprogramowania).	Obserwacja w warunkach symulowanych
Uczestnik potrafi monitorować status ochrony oraz reagować na incydenty bezpieczeństwa.	Identyfikacja i prawidłowa reakcja na przykładowe alerty w konsoli ESET PROTECT.	Obserwacja w warunkach symulowanych
Uczestnik zna metody zaawansowanego raportowania i analizowania danych w ESET PROTECT.	Sporządzenie raportu prezentującego wybrane dane z systemu ochrony.	Obserwacja w warunkach symulowanych
Uczestnik potrafi implementować uwierzytelnianie dwuskładnikowe i konfigurację zabezpieczeń dla zwiększenia bezpieczeństwa systemu.	Prawidłowa konfiguracja mechanizmów zabezpieczeń w środowisku testowym.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie 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

- 1. Informacje organizacyjne.
- 2. Konsole centralnego zarządzania ESET PROTECT on-prem i ESET PROTECT.
- 3. Ochrona stacji roboczych.
- 4. Wdrożenie agenta ESET PROTECT w systemie Linux.
- 5. Instalacja oprogramowania ESET ENDPOINT ANTIVIRUS w systemie Linux.
- 6. Uwierzytelnianie dwuskładnikowe do konsoli centralnego zarządzania.
- 7. Wykonywanie zaawansowanych zadań systemu operacyjnego.
- 8. ESET ENDPOINT ANTIVIRUS/SECURITY for Windows – zaawansowane polityki.
- 9. Rozwiązywanie problemów podczas wdrażania agenta ESET PROTECT.
- 10. Rozwiązywanie problemów podczas instalacji oprogramowania ESET ENDPOINT ANTIVIRUS/SECURITY.
- 11. Rozwiązywanie problemów połączeniowych agenta do serwera zdalnej administracji.
- 12. Wykorzystanie narzędzia ESET SysInspector.
- 13. Sesja pytań i odpowiedzi

Harmonogram

Liczba pozycji harmonogramu: 14

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Konsole centralnego zarządzania ESET PROTECT on-prem i ESET PROTECT.	Zajęcia	Paweł Kryński	06-11-2026	09:00	09:30	00:30
2 z 14 Ochrona stacji roboczych.	Zajęcia	Paweł Kryński	06-11-2026	09:30	10:00	00:30
3 z 14 Wdrożenie agenta ESET PROTECT w systemie Linux.	Zajęcia	Paweł Kryński	06-11-2026	10:00	10:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 14 Instalacja oprogramowania ESET ENDPOINT ANTIVIRUS w systemie Linux.	Zajęcia	Paweł Kryński	06-11-2026	10:30	11:00	00:30
5 z 14 -	Przerwa	-	06-11-2026	11:00	11:15	00:15
6 z 14 Uwierzytelnienie dwuskładnikowe do konsoli centralnego zarządzania.	Zajęcia	Paweł Kryński	06-11-2026	11:15	12:00	00:45
7 z 14 Wykonywanie zaawansowanych zadań systemu operacyjnego.	Zajęcia	Paweł Kryński	06-11-2026	12:00	12:45	00:45
8 z 14 ESET ENDPOINT ANTIVIRUS/SECURITY for Windows – zaawansowane polityki.	Zajęcia	Paweł Kryński	06-11-2026	12:45	13:30	00:45
9 z 14 -	Przerwa	-	06-11-2026	13:30	14:00	00:30
10 z 14 Rozwiązywanie problemów podczas wdrażania agenta ESET PROTECT.	Zajęcia	Paweł Kryński	06-11-2026	14:00	14:30	00:30
11 z 14 Rozwiązywanie problemów podczas instalacji oprogramowania ESET ENDPOINT ANTIVIRUS/SECURITY.	Zajęcia	Paweł Kryński	06-11-2026	14:30	15:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 14 Rozwiązywanie problemów połączeniowych agenta do serwera zdalnej administracji/ Wykorzystanie narzędzia ESET SysInspector.	Zajęcia	Paweł Kryński	06-11-2026	15:00	15:30	00:30
13 z 14 -	Przerwa	-	06-11-2026	15:30	15:45	00:15
14 z 14 -	Walidacja	-	06-11-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	07:00
w tym suma godzin zajęć	05:45
w tym suma godzin walidacji	00:15
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	08:00

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	2 447,70 PLN

Koszt przypadający na 1 uczestnika netto	1 990,00 PLN
Koszt osobogodziny brutto	349,67 PLN
Koszt osobogodziny netto	284,29 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	07:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Paweł Kryński

Trener techniczny i praktyk IT, specjalizujący się w cyberbezpieczeństwie oraz administracji rozwiązaniami ochrony endpointów. Prowadził szkolenia techniczne dla administratorów, w tym ESET Client & Network Security Administrator, ESET Inspect - Administrator XDR oraz ESET Advanced Administration, łącząc wiedzę teoretyczną z praktycznymi scenariuszami wdrożeniowymi. Wykształcenie wyższe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma:

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

Warunki uczestnictwa

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

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 niezminionej 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 i/lub MS Teams**

- 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) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

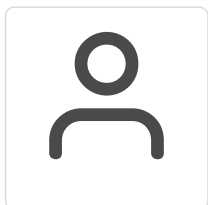
- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

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://szkolenia.dagma.eu/pl/training-list>

Kontakt



Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl

Telefon (+48) 327 931 015