



ESET - Protect Administrator

Numer usługi 2026/06/18/17164/3635114

3 677,70 PLN brutto

2 990,00 PLN netto

262,69 PLN brutto/h

213,57 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Dagma sp. z o.o.

★★★★☆ 4,5 / 5

460 ocen

📄 Usługa szkoleniowa

📺 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 14:00 h

📅 23.09.2026 do 24.09.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie jest skierowane do osób, które:

- **Pracują lub zamierzają pracować jako administratorzy systemów IT**, w szczególności odpowiedzialni za bezpieczeństwo i zarządzanie oprogramowaniem zabezpieczającym.
- **Chcą zdobyć praktyczne umiejętności w obsłudze i konfiguracji konsoli ESET PROTECT**, zarówno w wersji lokalnej (on-prem), jak i chmurowej.
- **Potrzebują wiedzy z zakresu zarządzania zabezpieczeniami stacji roboczych i serwerów** w środowiskach firmowych.
- **Planują wdrażać i utrzymywać rozwiązania ochrony przed zagrożeniami** oraz efektywnie je administrować w codziennej pracy.
- **Chcą poznać zaawansowane narzędzia i funkcje ESET**, takie jak polityki, grupy urządzeń, raportowanie, sandboxing czy szyfrowanie dysków.

Szkolenie i materiały w języku polskim.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

16-09-2026

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 edukacyjnym szkolenia jest przekazanie uczestnikom praktycznej wiedzy i umiejętności niezbędnych do samodzielnego wdrażania, konfiguracji oraz administracji platformą ESET PROTECT, umożliwiającą centralne zarządzanie bezpieczeństwem stacji roboczych i serwerów w środowisku firmowym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi wyjaśnić podstawowe zasady działania i architekturę ESET PROTECT	Poprawnie identyfikuje komponenty systemu i opisuje ich funkcje	Test teoretyczny
Uczestnik potrafi zainstalować i skonfigurować środowisko ESET PROTECT	Samodzielnie wykonuje instalację i wstępną konfigurację konsoli	Obserwacja w warunkach rzeczywistych
Uczestnik potrafi zarządzać urządzeniami oraz politykami bezpieczeństwa	Przypisuje urządzenia do grup i stosuje właściwe polityki ochrony	Obserwacja w warunkach rzeczywistych
Monitorować stan bezpieczeństwa i analizować zagrożenia	Poprawnie interpretuje alerty, zdarzenia i statusy ochrony	Obserwacja w warunkach rzeczywistych
Uczestnik potrafi reagować na incydenty oraz tworzyć raporty bezpieczeństwa	Podejmuje adekwatne działania administracyjne i generuje raporty	Obserwacja w warunkach rzeczywistych

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 wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Program

1. Informacje organizacyjne
2. Licencjonowanie
3. Konsole centralnego zarządzania ESET PROTECT on-prem i ESET PROTECT
4. Ochrona stacji roboczych
5. Grupy statyczne i dynamiczne
6. Zadania klienta i serwera
7. Wdrożenie agenta ESET PROTECT
8. Instalacja oprogramowania ESET SERVER SECURITY na serwerze
9. Zadania systemu operacyjnego
10. Polityki
11. Użytkownicy konsoli i zestawy uprawnień
12. Zagrożenia i wykrywanie
13. Wstrzymywanie ochrony, wyłączenia, wstrzymywanie polityk
14. Raportowanie
15. ESET ENDPOINT ANTIVIRUS/SECURITY for Windows – zaawansowane polityki
16. ESET MOBILE THREAT DEFENSE - ochrona urządzeń mobilnych Android i zarządzanie iOS
17. ESET RANSOMWARE REMEDIATION - autorska technologia przywracania plików po zaszyfrowaniu
18. ESET LIVE GUARD ADVANCED - sandboxing
19. ESET FULL DISK ENCRYPTION - szyfrowanie pełnej powierzchni dysku
20. Migracja ESET PROTECT on-prem do ESET Protect
21. Aktualizacja środowiska ESET
22. Wsparcie
23. Sesja pytań i odpowiedzi
24. Walidacja

Harmonogram

Liczba pozycji harmonogramu: 21

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Informacje organizacyjne	Zajęcia	Paweł Kryński	23-09-2026	09:00	09:15	00:15
2 z 21 Licencjonowanie / Konsole centralnego zarządzania ESET PROTECT on-prem i ESET PROTECT	Zajęcia	Paweł Kryński	23-09-2026	09:15	10:00	00:45
3 z 21 Ochrona stacji roboczych	Zajęcia	Paweł Kryński	23-09-2026	10:00	10:45	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 21 -	Przerwa	-	23-09-2026	10:45	11:00	00:15
5 z 21 Grupy statyczne i dynamiczne / Zadania klienta i serwera / Wdrożenie agenta ESET PROTECT	Zajęcia	Paweł Kryński	23-09-2026	11:00	13:30	02:30
6 z 21 -	Przerwa	-	23-09-2026	13:30	14:00	00:30
7 z 21 Instalacja oprogramowania ESET SERVER SECURITY na serwerze / Zadania systemu operacyjnego / Polityki / Użytkownicy konsoli i zestawy uprawnień	Zajęcia	Paweł Kryński	23-09-2026	14:00	15:15	01:15
8 z 21 -	Przerwa	-	23-09-2026	15:15	15:30	00:15
9 z 21 Zagrożenia i wykrywanie / Wstrzymywanie ochrony, wyłączenia, wstrzymywanie polityk / Raportowanie	Zajęcia	Paweł Kryński	23-09-2026	15:30	16:00	00:30
10 z 21 ESET ENDPOINT ANTIVIRUS/SECURITY for Windows – zaawansowane polityki	Zajęcia	Paweł Kryński	24-09-2026	09:00	10:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 21 ESET MOBILE THREAT DEFENSE - ochrona urządzeń mobilnych Android i zarządzanie iOS	Zajęcia	Paweł Kryński	24-09-2026	10:00	10:45	00:45
12 z 21 -	Przerwa	-	24-09-2026	10:45	11:00	00:15
13 z 21 ESET RANSOMWARE REMEDIATION - autorska technologia przywracania plików po zaszyfrowaniu	Zajęcia	Paweł Kryński	24-09-2026	11:00	11:30	00:30
14 z 21 ESET LIVE GUARD ADVANCED - sandboxing	Zajęcia	Paweł Kryński	24-09-2026	11:30	12:00	00:30
15 z 21 ESET FULL DISK ENCRYPTION - szyfrowanie pełnej powierzchni dysku	Zajęcia	Paweł Kryński	24-09-2026	12:00	13:00	01:00
16 z 21 -	Przerwa	-	24-09-2026	13:00	13:30	00:30
17 z 21 Migracja ESET PROTECT on-prem do ESET Protect	Zajęcia	Paweł Kryński	24-09-2026	13:30	14:15	00:45
18 z 21 Aktualizacja środowiska ESET	Zajęcia	Paweł Kryński	24-09-2026	14:15	14:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 21 Wsparcie / Sesja pytań i odpowiedzi	Zajęcia	Paweł Kryński	24-09-2026	14:45	15:30	00:45
20 z 21 -	Przerwa	-	24-09-2026	15:30	15:45	00:15
21 z 21 -	Walidacja	-	24-09-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:45
w tym suma godzin walidacji	00:15
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	16:00

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	3 677,70 PLN
Koszt przypadający na 1 uczestnika netto	2 990,00 PLN
Koszt osobogodziny brutto	262,69 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Paweł Kryński

Trener IT, prowadzący szkolenia w Dagma Szkolenia IT z zakresu cyberbezpieczeństwa. Specjalista z dziedziny rozwiązań ESET, prowadzący kursy z tematyki BlueTeam. Certyfikaty: Certified Ethical Hacker, Azure Fundamentals, Junior Penetration Tester, Certified ESET Inspect Optimization Specialist i wiele innych. 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 niezmięnionej łącznej liczby godzin usługi szkoleniowej.
- 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.
- 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

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



Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 327 931 093