Załącznik nr 1 do Zapytania ofertowego

Opis Przedmiotu Zamówienia

Oprogramowanie oraz infrastruktura sprzętowa

Projekt realizowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczne Wodociągi. Konkurs grantowy pn. "Cyberbezpieczne Wodociągi"

Spis Treści

I. WYMAGANIA OGÓLNE 5

1) Równoważność w zakresie Oprogramowania 5

2) Równoważność w zakresie Infrastruktury sprzętowej 6

II. OBSZAR TECHNICZNY IT 7

1. Platforma bezpieczeństwa łącząca oprogramowanie antywirusowe, oprogramowanie MDM, oprogramowanie EDR/XDR (IT/OT) 7

2. Oprogramowanie NDR wraz z dedykowaną platformą do zbierania i analizy ruchu sieciowego oraz HoneyPot dla usług sieciowych (IT/OT) 23

3. Wdrożenie rozwiązania SIEM (IT/OT) 26

4. Wdrożenie centralnego menadżera haseł w wersji on-premise (IT/OT) 27

5. Platforma bezpieczeństwa łącząca oprogramowanie ITSM, monitorowania infrastruktury informatycznej, zarządzać zasobami i licencjami, ITSM, SAM, CMDB (IT/OT) 31

6. Wdrożenie SoftHSM (IT/OT) 34

7. Wdrożenie infrastruktury klucza publicznego (IT/OT) 35

8. Urządzenie NGFW do Siedziby Głównej (IT/OT) 36

9. Serwer do stworzenia infrastruktury HA (IT/OT) 42

10. Urządzenie przeznaczone do stworzenia repozytorium kopii zapasowych (IT/OT) 47

11. Przełącznik dostępowy do Siedziby Głównej (IT/OT) 50

12. Przełącznik CORE do Siedziby Głównej (IT/OT) 51

13. Klucze U2F dla głównego administratora (IT/OT) 53

14. Szafa rack na urządzenia (IT/OT) 54

15. Access Point do Siedziby Głównej (IT/OT) 54

16. Audyt wraz z testami bezpieczeństwa infrastruktury sieciowej/sprzętowej (IT/OT) 55

17. Montaż i konfiguracja urządzeń UTM, przełączników aktualizacja do najnowszej wersji oprogramowania, wydzielenie vlanów, separacja sieci Wdrożenie oprogramowania XDR (IT/OT) 58

18. UPS dla serwerowni w Siedzibie Głównej (IT/OT) 59

19. UPS dla serwerowni (NAS) (IT/OT) 60

20. UPS dla stacji w Siedzibie Głównej - druga szafa (IT/OT) 61

21. Agregat z przyczepą transportową (IT/OT) 62

III. OBSZAR TECHNICZNY OT 65

1. Przełącznik do lokalizacji zdalnej (OT) 65

2. Sprzętowe sondy monitorujące w ramach systemu klasy IDS dla OT, umożliwiające bezpieczne oraz pasywne zbieranie kopii ruchu sieciowego (OT) 66

3. UPS dla lokalizacji zdalnej (OT) 69

4. Dedykowany dysk do przeprowadzania kopii zapasowych w środowiskach OT, które nie mają dostępu do sieci lokalnej/internetu (OT) 70

5. Urządzenie UTM dla lokalizacji zdalnych z ochroną protokołów przemysłowych (OT) 71

IV. OBSZAR KOMPETENCYJNY 76

1. Szkolenie dotyczące cyberbezpieczeństwa i cyberhigieny dla pracowników, działu IT oraz kadry zarządzającej poprzedzone symulowanymi atakiem phishingowym (IT/OT) 76
2. Szkolenie dla działu IT z rozwiązania NGFW, ITSM, XDR, System operacyjny serwera (IT/OT) 78

WSTĘP

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Szprotawskie Wodociągi i Kanalizacja Sp. z o.o. realizowanego w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczne Wodociągi. Konkurs grantowy pn. "Cyberbezpieczne Wodociągi".

Zamawiający wymaga, aby dostarczony sprzęt spełniający wymagania minimalne był fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w 2026 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished".

Celem przedsięwzięcia jest poprawa cyberbezpieczeństwa dla określonej grupy podmiotów krajowego systemu cyberbezpieczeństwa.

1) Równoważność w zakresie Oprogramowania

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, zapewnić gwarancję i serwis, uwzględnić niezbędną asystę ze strony pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Mając na uwadze powyższe, w przypadku jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności, przejrzystości, jawności a także równego traktowania wykonawców w trakcie prowadzenia postępowania, Zamawiający dopuszcza każdorazowo wymianę Oprogramowania u Zamawiającego pod warunkiem, że:

a) Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt, z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.

b) Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, w sposób opisany w niniejszym OPZ a migracja musi objąć pełny zakres danych bieżących i archiwalnych.

c) Wykonawca przeprowadzi instruktaże stanowiskowe, zapewni gwarancje i serwis gwarancyjny a także help desk oraz będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom Zamawiającego płynną obsługę Oprogramowania.

d) Wymiana Oprogramowania nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.

e) Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.

f) Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.

g) Nowe rozwiązania muszą realizować wszystkie wymienione wymagania względem Oprogramowania.

2) Równoważność w zakresie Infrastruktury sprzętowej

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

II. OBSZAR TECHNICZNY IT

1. Platforma bezpieczeństwa łącząca oprogramowanie antywirusowe, oprogramowanie MDM, oprogramowanie EDR/XDR (IT/OT)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Platforma bezpieczeństwa łącząca oprogramowanie antywirusowe, oprogramowanie MDM, oprogramowanie EDR/XDR (IT/OT)
Wymagania ogólne	W ramach dostawy Zamawiający wymaga dostarczenia wznowienia aktualnie posiadanej licencji na oprogramowanie antywirusowe ESET PROTECT Entry i podniesienia funkcjonalności posiadanej licencji do rozwiązania klasy EDR - ESET PROTECT ENTERPRISE. Dostarczone licencje muszą być ważne minimum do 31.12.2026 r. Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo: W ramach dostawy Zamawiający wymaga dostarczenia, wdrożenia oraz zapewnienia wsparcia technicznego dla kompleksowego oprogramowania antywirusowego do ochrony stacji roboczych i serwerów w środowisku teleinformatycznym Zamawiającego. Rozwiązanie ma zapewniać zaawansowaną ochronę przed zagrożeniami cybernetycznymi, przed złośliwym oprogramowaniem, atakami ukierunkowanymi, zagrożeniami zero-day. Oprogramowanie musi łączyć klasyczne mechanizmy ochrony antywirusowej z funkcjonalnościami klasy EDR. Dostarczona licencja musi pozwalać na instalację oprogramowania na minimum 26 urządzeniach (komputerach i serwerach). Dostarczone licencje muszą być ważne do 31.12.2026 r.
Centralne zarządzanie	1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS). 2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim. 3. Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania. 4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS. 5. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID. 6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory. 7. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji. 8. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej: • Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a

	serwerem centralnego zarządzania. • Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta. • Buforowanie ruchu HTTPS. 9. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania. 11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android: • Google Authenticator, • Microsoft Authenticator, • Authy, • Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania. 12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora. 13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 14. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: • Adresy sieciowe IP. • Aktywne zagrożenia. • Stan funkcjonowania oraz ochrony. • Wersja systemu operacyjnego. • Podzespoły komputera. 15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem: • Wyrażenie CRON. • Codziennie. • Cotygodniowo. • Co miesiąc. • Co rok. • Po wystąpieniu nowego zdarzenia. • Po automatycznym umieszczeniu hosta w grupie dynamicznej. 16. Rozwiązanie musi udostępniać możliwość tagowania obiektów. 17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog. 18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach: • JSON. • LEEF. • CEF.
Ochrona stacji roboczych- Windows	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim. 3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: • Wirus.

	• Trojan. • Robak. • Adware. • Spyware. • Dialer. • Phishing. • Backdoor. 4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się. 6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet. 7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware. • Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych. • Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service). • Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy. 8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: • Całego dysku. • Wybranych katalogów. • Pojedynczych plików. • Plików spakowanych oraz skompresowanych. • Dysków sieciowych. • Dysków przenośnych. 11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: • Wybranych plików. • Wybranych procesów. • Wybranych lokalizacji. • Wybranych rozszerzeń. • Nazwy wykrycia. • Sumy kontrolnej (SHA1). 12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology. 13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej: • Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego. • Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników. • Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

	14. Rozwiązanie musi udostępniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS. 16. Rozwiązanie musi udostępniać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej: A. Typ urządzenia: • Pamięci masowe. • Optyczne pamięci masowe. • Pamięci masowe Firewire. • Urządzenia do tworzenia obrazów. ○ Drukarki USB. ○ Urządzenia Bluetooth. ○ Czytniki kart inteligentnych. ○ Modemy. ○ Porty LPT/COM. ○ Urządzenia przenośne. B. Parametry urządzenia: • Numer seryjny. • Producent. • Model. C. Typ dostępu: • Brak możliwości zapisu. • Pełen dostęp • Ostrzeżenie użytkownika. • Brak dostępu. 18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji. • Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa

	• Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. • Raport musi posiadać co najmniej: ○ Listę zainstalowanych aplikacji. ○ Listę usług systemowych. ○ Informacje o systemie operacyjnym i sprzęcie. ○ Listę aktywnych procesów i połączeń sieciowych. ○ Harmonogram systemu operacyjnego. ○ Szczegóły pliku hosts. ○ Informacje o sterownikach. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: • Antywirus. • Zapora osobista. • Sandbox. • Antyspyware. • Metody heurystyczne. 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę. A. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook. B. Ochrona musi być realizowana w oparciu o co najmniej: • globalna czarna lista RBL, • czarna lista użytkownika, • biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook. 23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności: A. Ochrona przed anomaliami sieciowymi, w tym co najmniej: B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta. B. Zapora osobista musi posiadać co najmniej cztery tryby pracy: • tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu. 25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.

	• Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. • Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. • W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu. 26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta. A. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii. B. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: • Treść komunikatu. • Obraz.
Ochrona stacji roboczych MacOS	1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych. 2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: • Wirus. • Trojan. • Robak. • Adware. • Spyware. • Dialer. • Phishing. • Backdoor. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 6. Rozwiązanie musi chronić pliki co najmniej za pomocą: • Sygnatur wirusów. • Reputacji chmurowej. 7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej: • Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu. • Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników. • Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. 9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu

	kontekstowego oraz zgodnie z harmonogramem co najmniej: • całego dysku, • wybranych katalogów, • pojedynczych plików, • plików spakowanych oraz skompresowanych, • Dysków sieciowych, • dysków przenośnych. 10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: • wybranych plików, • wybranych procesów, • wybranych lokalizacji, • wybranych rozszerzeń, • nazwy wykrycia, • sumy kontrolnej (SHA1). 11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta. B. Zapora osobista musi posiadać co najmniej dwa tryby pracy: ○ tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, ○ tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
Ochrona stacji roboczych- Linux	1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: • Ubuntu Desktop, • Red Hat Enterprise Linux • Linux Mint. 2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu: • Cinnamon. • GNOME. • KDE. • MATE. • XFCE. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: • Wirus. • Trojan. • Robak. • Adware. • Spyware. • Dialer. • Phishing. • Backdoor. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania

	antywirusowego, który umożliwia co najmniej: • Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników. • Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. 7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: • Całego dysku. • Wybranych katalogów. • Pojedynczych plików. • Plików spakowanych oraz skompresowanych. • Dysków sieciowych. • Dysków przenośnych. 8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: • Wybranych plików. • Wybranych procesów. • Wybranych lokalizacji. • Wybranych rozszerzeń. 9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej: A. typ urządzenia: ○ pamięci masowe, ○ optyczne pamięci masowe, B. parametry urządzenia: ○ numer seryjny, ○ producent, ○ model. C. typ dostępu: ○ brak możliwości zapisu, ○ pełen dostęp, ○ brak dostępu.
Ochrona serwera-Windows Server	1. Rozwiązanie musi wspierać systemy w tym co najmniej: • Microsoft Windows Server 2012 R2, • Microsoft Windows Server 2016, • Microsoft Windows Server 2019, • Microsoft Windows Server 2022, • Microsoft Windows Server 2025. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: • Wirus. • Trojan. • Robak. • Adware. • Spyware. • Dialer. • Phishing. • Backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły

	heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej: • Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego. • Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników. • Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. 9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: • całego dysku, • wybranych katalogów, • pojedynczych plików, • plików spakowanych oraz skompresowanych, • dysków sieciowych, • dysków przenośnych. 10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: • wybranych plików, • wybranych procesów, • wybranych lokalizacji, • wybranych rozszerzeń, • nazwy wykrycia, • sumy kontrolnej (SHA1). 11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji. A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i

	mogą stanowić zagrożenie bezpieczeństwa. B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. C. Raport musi posiadać co najmniej: ○ Listę zainstalowanych aplikacji, ○ Listę usług systemowych, ○ Informacje o systemie operacyjnym i sprzęcie, ○ Listę aktywnych procesów i połączeń sieciowych, ○ harmonogram systemu operacyjnego, ○ Szczegóły pliku hosts, ○ Informacje o sterowników. 14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: • antywirus, • zapora osobista • sandbox, • antyspyware, • metody heurystyczne. 15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V. 16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej: A. typ urządzenia: ○ Pamięci masowe. ○ Optyczne pamięci masowe. ○ Pamięci masowe Firewire. ○ Urządzenia do tworzenia obrazów. ○ Drukarki USB. ○ Urządzenia Bluetooth. ○ Czytniki kart inteligentnych. ○ Modemy. ○ Porty LPT/COM. ○ Urządzenia przenośne. B. parametry urządzenia: ○ Numer seryjny, ○ Producent, ○ Model. C. typ dostępu: ○ Brak możliwości zapisu, ○ Pełen dostęp, ○ Ostrzeżenie użytkownika, ○ Brak dostępu. 18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług: • MS SQL. • Active Directory. • IIS. • Sysvol.

	• DNS. • DHCP. • Hyper-V. • Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego. 19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności: A. Ochrona przed anomaliami sieciowymi, w tym co najmniej: B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. 21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta. A. Zapora osobista musi posiadać co najmniej cztery tryby pracy: ○ tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, ○ tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, ○ tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący, ○ tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
Ochrona serwera-Linux	1. Rozwiązanie musi wspierać systemy w tym co najmniej: • RedHat Enterprise Linux (RHEL), • Rocky Linux, • Ubuntu, • Debian, • SUSE Linux Enterprise Server (SLES), • Oracle Linux, • Amazon Linux. 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: • Wirus. • Trojan. • Robak. • Adware. • Spyware. • Dialer. • Phishing. • Backdoor. 3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS. 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

	6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej: • Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników. • Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy. 8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: • całego dysku, • wybranych katalogów, • pojedynczych plików, • plików spakowanych oraz skompresowanych, • dysków sieciowych, • dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: • wybranych plików, • wybranych procesów, • wybranych lokalizacji, • wybranych rozszerzeń, 10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. • Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. 13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach: • proces budowania obrazu kontenera, • wdrażanie obrazu kontenera.
Mobilne Device Management	1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania. A. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: ○ Android, ○ iOS, ○ iPadOS. B. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami: ○ Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników), ○ Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

	○ VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), ○ Apple Business Manager (ABM), ○ Android Enterprise (co najmniej w zakresie Device Owner). 3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: • usunięcie zawartości urządzenia, • przywrócenie urządzenia do ustawień fabrycznych, • zablokowanie urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS, • Resetowanie hasła blokady ekranu. 4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 5. MDM musi umożliwiać co najmniej: A. Dla systemów iOS oraz iPadOS: ○ konfigurację kont e-mail, ○ konfigurację połączeń VPN, ○ Konfigurację połączeń Wi-Fi, ○ Konfigurację listy certyfikatów, ○ możliwość uruchomienia trybu jednej aplikacji. B. Dla systemu Android: ○ blokadę wykonywania połączeń, ○ blokadę konfiguracji sieci Wi-Fi, ○ blokadę konfiguracji tuneli VPN, ○ zarządzenie aktualizacjami sytemu operacyjnego, ○ blokadę zmiany tapety urządzenia.
Mobile Threat Defense (MTD) dla system Android	1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: • Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD. • Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej: A. Złożoność kodu blokady ekranu: ○ Wzór. ○ PIN. ○ Hasło. B. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu, C. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu. 5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła. 6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze	1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń. 2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. 3. Rozwiązanie musi wspierać systemy w tym co najmniej: 4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego. 6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej: 7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej: 8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia. 11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu. 13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników: 14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej: 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.
Szyfrowanie	1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego. 2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker. 3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego. 5. Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. • Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia. • Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania. 6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania. • Hasło odzyskiwania po użyciu musi zostać zmodyfikowane. • Hasło odzyskiwania nie może być krótsze niż 8 znaków. • Hasło odzyskiwania nie może być dłuższe niż 20 znaków. 7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

	8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory. 9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0. 10. Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0. 11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku. 12. Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia w przypadku aktualizacji systemu operacyjnego.
Endpoint Detection and Response / eXtended Detection and Response	1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego. 2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego. 3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego: • Tworzenie procesów. • Uruchamianie, zatrzymanie i modyfikacja usług. • Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym. • Usuwanie oraz zmiana nazw plików. • Tworzenie i usuwanie kluczy rejestru systemowego. • Ładowanie bibliotek DLL. • Zalogowanie użytkowników. A. Elementy sieciowe, w tym co najmniej: ○ Pobranie plików wykonywalnych. ○ Zestawienie połączeń TCP/IP. ○ Zapytania http. ○ Zapytania DNS. 4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. A. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach: ○ Blokowanie pliku wykonywalnego. ○ Blokowanie pliku wykonywalnego i poddanie go kwarantannie. ○ Blokowanie podejrzanej biblioteki DLL. ○ Zakończenie procesu. ○ Skanowanie komputera w poszukiwaniu zagrożeń. ○ Wyłączenie komputera. ○ Izolacja sieciowa hosta dla systemów Windows oraz Linux. ○ Wylogowanie użytkownika. B. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML. 5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. A. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia. B. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:

	○ Proces. ○ Proces nadrzędny (proces rodzica). ○ Nazwę procesu. ○ Ścieżkę procesu. ○ Wiersz polecenia. ○ Wydawcę. ○ Typ podpisu cyfrowego. ○ SHA-1. ○ SHA-2. ○ Użytkownika. C. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML. 6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych. A. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku. B. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące): ○ SHA-1. ○ SHA-256. 7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej: • Hash pliku SHA-1. • Hash pliku SHA-256. • Hash pliku MD5. • Typ sygnatury podpisu cyfrowego. • Wydawcę certyfikatu. • Wersję pliku. • Oryginalną nazwę pliku. • Rozmiar pliku. • Reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego. • Pierwsze uruchomienie pliku w środowisku. • Ostatnie uruchomienie pliku w środowisku. 8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL: • Oznaczania ich jako bezpieczne lub niebezpieczne. • Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, • Zablokowania wykonywania i wykorzystania pliku. • Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego. 9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń). • Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. • Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, • Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego. • Administrator musi posiadać możliwość szczegółowego podglądu

	wykonanych przez skrypt czynności w formie tekstowej. • Administrator musi posiadać możliwość odczytania informacji o języku skryptu. 10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera. • Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli. 11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów. 12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal. 13. Rozwiązanie musi umożliwiać moduł zaawansowanego wyszukiwania, które umożliwia badanie wskaźników danych zawartych w XDR, przynajmniej w oparciu o: • Wyszukiwanie dowolnego tekstu. • Wyszukiwanie, pozwalające łączyć ze sobą różne słowa, oddalone od siebie nie więcej niż 3 innymi słowami. • Wyszukiwanie po nazwie procesów. • Wyszukiwanie po ocenie ryzyka. • Filtrowanie według daty.
Wsparcie techniczne	Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji. Licencje muszą być ważne do 31.12.2026
Ilość	1 szt.

2. Oprogramowanie NDR wraz z dedykowaną platformą do zbierania i analizy ruchu sieciowego oraz HoneyPot dla usług sieciowych (IT/OT)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie NDR wraz z dedykowaną platformą do zbierania i analizy ruchu sieciowego oraz HoneyPot dla usług sieciowych (IT/OT)
Wymagania ogólne	Zamawiający oczekuje dostarczenia, wdrożenia i uruchomienia systemu klasy Network Detection and Response (NDR) służącego do pasywnej analizy ruchu sieciowego, wykrywania zagrożeń bezpieczeństwa oraz wspomagania reagowania na incydenty cyberbezpieczeństwa z dedykowaną platformą sprzętową.
System NDR	System NDR musi umożliwiać: • ciągłe monitorowanie ruchu sieciowego w sieci lokalnej, • analizę komunikacji wewnętrznej (east–west) oraz komunikacji z sieciami zewnętrznymi (north–south), • wykrywanie anomalii i zdarzeń mogących świadczyć o naruszeniu bezpieczeństwa, • wsparcie administratorów i zespołów bezpieczeństwa w identyfikacji oraz analizie incydentów.
Wymagania funkcjonalne NDR	System musi spełniać co najmniej następujące wymagania funkcjonalne: 1. Wykrywanie i reagowanie: ○ Ocena ryzyka, ○ Zarządzanie ryzykiem,

	○ Analiza zagrożeń, ○ Polityki informowania o ryzyku, ○ Pułapki na cyberataki, ○ Wykluczenia, ○ Monitorowanie portów, ○ Powiadomienia o zdarzeniach, ○ Nadawca dziennika, ○ Kwarantanna, ○ Reguły ochrony, 2. Zarządzanie siecią: ○ Obsługa ramek Jumbo, ○ Obsługa VLAN, ○ Konfiguracja IP, 3. Przestrzeń dyskowa: ○ Pojemność systemu, ○ Wolumin aplikacji, ○ Typ RAID, ○ Informację o dysku i informacje SMART, ○ Test SMART dysku i harmonogram testu SMART, ○ Skanowanie I odzyskiwanie uszkodzonych bloków na dysku, 4. Zarządzanie dziennikami: ○ Dziennik zdarzeń, ○ Dziennik dostępu, ○ Użytkownicy online, ○ Ustawienia wpisów dziennika, ○ Ustawienia czasu przechowywania dziennika, ○ Ustawienia języka dziennika, ○ Nadawca dziennika, ○ Odbiorca dziennika, 5. Monitor zasobów: ○ Zasoby systemowe- procesor/pamięć/sieć, ○ Zasoby pamięci masowej, ○ Wykorzystywanie woluminów/stanu/pamięci masowej, ○ Aktywność procesów. 6. Zabezpieczenia: ○ Certyfikat i klucz prywatny, ○ Wymiana certyfikatu i pobieranie certyfikatu, ○ Zasady dotyczące haseł, ○ Reguła siły hasła, ○ Reguła okresowej zmiany hasła, ○ Ochrona systemu przed manipulacjami, ○ Kontrola bezpieczeństwa. 7. Zarządzanie systemem: ○ Ustawienia ogólne, ○ Sprzęt, ○ Zasilanie, ○ Aktualizacja systemu, ○ Kopia zapasowa/przywracanie, ○ UPS, ○ Status systemu, ○ Uprawienia, ○ Zarządzanie użytkownikami, ○ Serwer SSH,

	○ Usługa SNMP (V1/V2/V3) ○ Usługa wykruwania UPnP 8. Obsługiwane klienckie systemy operacyjne: ○ Apple Mac OS 10.7 ○ Linux ○ Unix, ○ Microsoft Windows 7, 8, 10, 11 lub nowsze, ○ Microsoft Windows Server 2003, 2008 R2, 2012, 2012 R2, 2016, 2022 lub nowsze 9. Wspierane przeglądarki: ○ Apple Safari 7 lub nowsze, ○ Google Chrome, ○ Microsoft Internet Explorer 10 lub nowsze, ○ Mozilla Firefox,
Specyfikacja techniczna platformy	System NDR musi zostać dostarczony na dedykowanej z wbudowanymi zasobami obliczeniowymi, spełniającej co najmniej poniższe wymagania: 1. Procesor: co najmniej 4-rdzeniowy procesor o taktowanie nie mniejszym niż 2,2Ghz 2. Architektura procesora: 64-bitowy x86 3. Pamięć RAM: co najmniej 8GB SODIMM DDR4 4. Możliwość rozbudowy RAM: co najmniej do 64GB 5. Obsługa dysków: co najmniej 2 dyski 2,5-calowe SATA 6 Gb/s, 3GB/s oraz 2 dyski NVMe, PCIe Gen 3 x 1 6. Liczba wszystkich portów: co najmniej 18 7. Liczba portów 10GbE SFP+: co najmniej 2 8. Liczba portów 2.5GbE (RJ45): co najmniej 8 9. Liczba portów 1GbE (RJ45): co najmniej 8 10. Złącza PCIe: co najmniej 2 PCIe Gen 3 11. Porty USB 3.2: co najmniej 2 12. Porty do zarządzania: co najmniej 4 13. Tabela adresów MAC: co najmniej 32K, 14. Łączna przepustowość nieblokująca: co najmniej 48Gbps 15. Zdolność przełączania: co najmniej 96Gbps 16. Typ zarządzania: przez przeglądarkę – sieć WEB 17. Obsługa norm: ○ IEEE 802.3u 100Tx Fast Ethernet ○ IEEE 802.3ab 1000BASE-T Gigabit Ethernet ○ IEEE 802.3bz 2.5G/5G BASE-T Multi-Gig Ethernet ○ IEEE 802.3an 10GBASE-T 10G Ethernet ○ IEEE 802.3ae 10GBASE-SR ○ IEEE 802.3ae 10GBASE-LR ○ IEEE 802.3z 1000Base-X ○ IEEE 802.3x Kontrola przepływu w pełnym dupleksie ○ IEEE 802.1q Wirtualne sieci LAN (VLAN) ○ IEEE 802.1p Protokół QoS dla priorytetyzacji ruchu 18. Obudowa: Rack, 1U 19. Wyświetlacz: Wymagany na przednim panelu urządzenia 20. Obsługiwane systemy plików: co najmniej EXT3, EXT4, NTFS, FAT32, HFS+ 21. Urządzenie musi zostać dostarczone wraz z minimum 2 dyskami klasy SSD o pojemności minimum 250GB.
Systemy	System musi mieć możliwość zainstalowania jednocześnie dwóch systemów

operacyjne	operacyjnych. Pierwszy z nich musi umożliwiać testowanie i badanie sieci, musi posiadać funkcje wykrywania, analizy i reagowania na zdarzenia występujące w sieci. Aplikacja powinna posiadać możliwość wykrywania oprogramowania ransomware w sieciach lokalnych lub blokować podejrzane działania, aby pomóc w zapobieganiu wyciekom poufnych danych i ograniczaniu rozprzestrzeniania się oprogramowania ransomware w sieci lokalnej. System powinien umożliwiać zainstalowanie drugiego, odrębnego systemu, który będzie umożliwiał przechowywanie plików. System musi umożliwiać również tworzenie oraz uruchamianie maszyn wirtualnych/kontenerów. Jeśli do działania systemu są potrzebne jakiekolwiek licencje – muszą one być zawarte w ofercie. Awaria jednego z systemów, nie może mieć żadnego wpływu na drugi system.
Gwarancja	Zamawiający wymaga, aby system minimum 12 miesięczną gwarancję wraz ze wsparciem producenta obejmującym dostęp do stabilnych wersji oprogramowania oraz wsparcia technicznego.
Ilość	1 szt.

3. Wdrożenie rozwiązania SIEM (IT/OT)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Wdrożenie rozwiązania SIEM (IT/OT)
Wymagania ogólne	W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta. Rozwiązanie musi umożliwiać logowanie się za pomocą konta ActiveDirectory, lub LDAP. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS. Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder). Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.), na podstawie zaawansowanych zapytań tworzonych między innymi za pomoca operatorów AND/OR Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne oraz budowanie własnych dashboardów.

	Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP). Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów) Rozwiązanie musi umożliwiać archiwizację logów i określać ich retencję. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV. Rozwiązanie musi umożliwiać tworzenie statycznych raportów. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów. Rozwiązanie musi umożliwiać tworzenie własnych raportów. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań oraz zarządzanie incydentami poprzez możliwość podglądu logów źródłowych zawartych w incydencie.
Wdrożenie	Zamawiający wymaga wdrożenia w zakresie minimum: • Instalacja i konfiguracja systemu operacyjnego (lub import gotowej spreparowanej maszyny) • Instalacja i konfiguracja oprogramowania; • Instalacja przy udziale Zamawiającego, agentów na komputerach z systemem Windows oraz Linux posiadanych przez Zamawiającego; • Konfiguracja urządzeń sieciowych przy udziale Zamawiającego, tj. wysyłania logów SYSLOG z urządzeń do serwera oraz konfiguracja ich przetwarzania; • Konfiguracja kopii zapasowych do wyznaczonego udziału SMB Zamawiającego • Weryfikacja poprawnej pracy systemu; • Przekazanie Zamawiającemu danych dostępowych do pulpitu nawigacyjnego (dashboard)
Administracja Systemem	Weryfikacja poprawności wykonywania kopii zapasowych SIEM; Aktualizacja oprogramowania systemowego oraz SIEM; Przekazywanie monitów za pomocą panelu nawigacyjnego (dashboard) SIEM; Raportowanie okresowe.
Ilość	1 szt.

4. Wdrożenie centralnego menadżera haseł w wersji on-premise (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Wdrożenie centralnego menadżera haseł w wersji on-premise (IT/OT)
Wymagania ogólne	Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego, oprogramowania zarządzanego menedżera haseł z możliwością udostępniania i współpracy w zakresie wymiany danych dostępowych. Minimalne wymagania ogólne: 1. Oprogramowanie musi umożliwiać zarządzanie danymi dostępowymi do zewnętrznych usług w postaci minimum loginu i hasła oraz adresu URL strony.

	2. Licencja powinna pozwalać na korzystanie z oprogramowania przez minimum 20 użytkowników. Zamawiający wymaga licencji bezterminowych, wsparcie musi obowiązywać do daty minimum 31.12.2026 3. Oprogramowanie musi umożliwić przechowywanie nieograniczonej ilości wpisów z danymi dostępowymi. 4. Oprogramowanie musi przechowywać wszystkie dane (dane użytkowników wraz z wpisami) na serwerze Zamawiającego. 5. Oprogramowanie musi udostępniać opcję dedykowanej pomocy technicznej w języku polskim z możliwością zgłaszania problemów w portalu poprzez wypełnienie formularza, składającego się min. z tytułu, treści oraz ewentualnych załączników. 6. Oprogramowanie musi być dostępne w języku polskim i angielskim z możliwością zmiany języka z poziomu organizacji oraz indywidualnego użytkownika. 7. Oprogramowanie musi posiadać ocenę A+ pod względem ustawionych nagłówków HTTP względem strony https://securityheaders.com/, tj. ustawiony nagłówek Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options, Refferer-Policy, Permission-Policy oraz Content-Security-Policy. 8. Oprogramowanie musi posiadać architekturę klient/serwer z umożliwieniem uruchomienia jej w opcji on-premise. 9. Oprogramowanie musi spełniać normy dostępności treści internetowych dla osób niepełnosprawnych min. w zakresie wyboru kroju czcionki, wyboru rozmiaru czcionki oraz możliwości czytania tekstu. Minimalne wymagania dotyczące przechowywania haseł: 1. Oprogramowanie musi umożliwić tworzenie, modyfikowanie i usuwanie wpisów z danymi dostępowymi składającymi się z minimum: • Tytułu, • Loginu, • Hasła, • Adresu URL strony, • Daty wygaśnięcia, • Notatki. 2. Oprogramowanie musi umożliwić dodawanie wpisów z danymi dostępowymi bez konieczności podawania wszystkich pól wymienionych w punkcie 1. 3. Oprogramowanie musi umożliwić nadawanie etykiet na wpisy, umożliwiając przy tym wizualną identyfikację przynależności do danej etykiety. 4. Oprogramowanie musi umożliwić dodawanie załączników do wpisów w formie plików z możliwością zdefiniowania dozwolonych rozszerzeń i rozmiarów w licencji. 5. Oprogramowanie musi umożliwić tworzenie grup dostępowych, szyfrowanych w myśl zasady zero-knowledge, tj. zaszyfrowanych na każdym etapie transferu danych z serwera do użytkownika i na odwrót i możliwych do odszyfrowania jedynie przez użytkownika lub odbiorcę. 6. Oprogramowanie musi umożliwić dostosowywanie grup dostępowych poprzez nazwy oraz ikony. 7. Oprogramowanie musi umożliwić możliwość tworzenia grup prywatnych, do których dostęp ma jedynie właściciel. 8. Oprogramowanie musi umożliwić tworzenie grup współdzielonych, do których dostęp ma właściciel i wszyscy uprawnieni użytkownicy wskazani przez właściciela. 9. Oprogramowanie musi mieć możliwość wyszukiwania wpisów po tytule. 10. Oprogramowanie musi posiadać wbudowany generator haseł

	umożliwiający definiowanie złożonych haseł o określonej długości z możliwością dostosowania występowania wielkich liter, małych liter, cyfr oraz symboli i wykluczenia konkretnych znaków. 11. Oprogramowanie musi wskazywać na ile bezpieczne jest wygenerowane hasło pod kątem jego entropii. 12. Oprogramowanie musi umożliwiać udostępnianie haseł w obrębie organizacji wykorzystując mechanizm grup współdzielonych. 13. Oprogramowanie musi umożliwiać import haseł z innych menedżerów haseł, minimum: • Google Chrome, • Mozilla Firefox, • Apple Safari, • KeePass. 14. Oprogramowanie musi udostępniać możliwość przeglądania załączników do haseł za pomocą dedykowanego widoku na portalu. Minimalne wymagania dotyczące zarządzania użytkownikami i przywilejami: 1. Oprogramowanie musi umożliwiać zarządzanie użytkownikami w ramach licencji w formie tworzenia, edycji oraz usuwania. 2. Oprogramowanie musi udostępniać konto właściciela, kierowników oraz normalnych użytkowników. 3. Oprogramowanie musi umożliwiać nadawanie dostępu do całych grup współdzielonych w formie opcji zapisu lub read-only (tylko do odczytu). 4. Oprogramowanie musi umożliwiać nadawanie dostępu do poszczególnych wpisów w grupach współdzielonych w formie opcji zapisu lub read-only (tylko do odczytu). 5. Oprogramowanie musi umożliwiać dostęp do danych na temat aktywności użytkowników. 6. Oprogramowanie musi umożliwiać dostęp do raportów o ujawnionych hasłach w wyniku wycieków danych logowania. 7. Oprogramowanie musi udostępniać ogólny wskaźnik siły haseł dla administratorów. 8. Oprogramowanie musi umożliwiać nadawanie miękkich wymagań na hasła z grup współdzielonych oraz wyświetlać ewentualne naruszenia w panelu administratora. 9. Oprogramowanie musi umożliwiać nadawanie i odbieranie przywilejów do tworzenia grup współdzielonych i/lub personalnych dla użytkowników. 10. Oprogramowanie musi umożliwiać dostęp do logów systemowych, zbierających informacje o aktywności użytkowników w zakresie minimum: • Aktywacji konta, • Logowania, • Tworzenia/modyfikacji/usuwania grup/wpisów. 11. Oprogramowanie musi umożliwiać eksport logów do formatu .csv z możliwością definicji zakresu czasowego, typu logów czy użytkownika, którego dotyczą. Minimalne wymagania dotyczące szyfrowania: 1. Oprogramowanie musi umożliwiać nadanie dwóch haseł użytkownika, jedno do konta, drugie do szyfrowania/odszyfrowania danych. 2. Oprogramowanie musi umożliwiać zmianę i reset hasła do konta. 3. Oprogramowanie musi stosować funkcję PBKDF2 na poziomie minimum 800000 iteracji. 4. Oprogramowanie musi stosować szyfrowanie symetryczne oraz

	asymetryczne w procesie zabezpieczania wpisów z hasłami, wykorzystując klucze RSA o długości minimum 2048 bitów oraz szyfrowania AES w trybie GCM. 5. Oprogramowanie musi umożliwić użytkownikowi nadania sobie weryfikacji dwuetapowej w postaci minimum: • Kodu SMS, • Kodu e-mail, • Kodu w aplikacji zewnętrznego dostawcy (np. Google Authenticator, Microsoft Authenticator), • Sprzętowych kluczy zabezpieczających. Minimalne wymagania dotyczące wtyczki do przeglądarki: 1. Oprogramowanie musi umożliwić pobranie i uruchomienie wtyczki w przeglądarkach minimum: • Google Chrome, • Mozilla Firefox, • Apple Safari. 2. Oprogramowanie w postaci wtyczki musi obsługiwać logowanie za pomocą tych samych kont co na portalu WWW. 3. Oprogramowanie musi umożliwiać obsługę weryfikacji dwuetapowej 2FA. 4. Oprogramowanie musi umożliwiać dodawanie wpisów wewnątrz wtyczki. 5. Oprogramowanie musi umożliwiać automatyczne proponowanie dodawania wpisów w przypadku wykrycia logowania na nowym portalu. 6. Oprogramowanie musi umożliwiać przeglądanie posiadanych wpisów wraz z możliwością kopiowania poszczególnych danych. 7. Oprogramowanie musi posiadać wbudowany generator haseł umożliwiający definiowanie złożonych haseł o określonej długości z możliwością dostosowania występowania wielkich liter, małych liter, cyfr oraz symboli i wykluczenia konkretnych znaków. 8. Oprogramowanie musi umożliwiać aktualizację wpisów w przypadku wykrycia zmiany hasła na portalu. 9. Oprogramowanie musi umożliwiać funkcjonalność automatycznego wypełniania pól formularza logowania za pomocą nakładki loginem i hasłem dodanym wcześniej do banku haseł. Minimalne wymagania dotyczące aplikacji mobilnej: 1. Oprogramowanie musi umożliwić pobranie i uruchomienie aplikacji na systemach mobilnych w sklepach: • Google Play na urządzenia mobilne z systemem Android, • Apple AppStore na urządzenia mobilne z systemem iOS. 2. Oprogramowanie w postaci aplikacji mobilnej musi obsługiwać logowanie za pomocą tych samych kont co na portalu WWW. 3. Oprogramowanie musi umożliwiać obsługę weryfikacji dwuetapowej 2FA. 4. Oprogramowanie musi umożliwiać dodawanie wpisów wewnątrz aplikacji mobilnej. 5. Oprogramowanie musi umożliwiać przeglądanie posiadanych wpisów wraz z możliwością kopiowania poszczególnych danych. 6. Oprogramowanie musi posiadać wbudowany generator haseł umożliwiający definiowanie złożonych haseł o określonej długości z możliwością dostosowania występowania wielkich liter, małych liter, cyfr oraz symboli i wykluczenia konkretnych znaków. Minimalne wymagania dotyczące wdrożenia i obsługi: 1. Instalacja komponentów na wskazanym serwerze (lub maszynie

	wirtualnej) 2. Podstawowa konfiguracja oraz utworzenie konta głównego administratora systemu 3. Weryfikacja poprawności instalacji i wykonanie testów uruchomieniowych Wykonawca zapewni szkolenie w zakresie użytkowania i administrowania wdrożonego systemu. Szkolenie ma zostać przeprowadzone dla minimum 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.
Ilość	1 szt.

5. Platforma bezpieczeństwa łącząca oprogramowanie ITSM, monitorowania infrastruktury informatycznej, zarządzać zasobami i licencjami, ITSM, SAM, CMDB (IT/OT)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Platforma bezpieczeństwa łącząca oprogramowanie ITSM, monitorowania infrastruktury informatycznej, zarządzać zasobami i licencjami, ITSM, SAM, CMDB (IT/OT)
Wymagania ogólne	Przedmiotem zamówienia jest modularne oprogramowanie do zarządzania infrastrukturą IT z możliwością obsługi inwentaryzacji zasobów, monitoringu użytkowników, ochrony danych oraz obsługi zgłoszeń związanych z pomocą techniczną dla użytkowników. System musi składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy serwerem, agentami i konsolami musi być w pełni szyfrowana za pomocą protokołu TLS 1.3.
Bezpieczeństwo i zgodność	Oprogramowanie musi dostarczać rozbudowane mechanizmy bezpieczeństwa, w tym minimum: 1. Uwierzytelnianie i dostęp: • Logowanie administratorów z dwuskładnikowym uwierzytelnianiem MFA (SMS/e-mail). • Rozbudowany system ról i poziomów uprawnień do funkcji oraz danych (w tym danych osobowych). • Szczegółowy dziennik operacji administratorów, z możliwością wysyłania logów do zewnętrznego systemu Syslog. • Synchronizacja z Active Directory (w tym atrybuty i awatary) z opcją LDAPS. 2. Ochrona przed ingerencją • Agent zabezpieczony przed usunięciem nawet przez lokalnych administratorów. • Instalator podpisany cyfrowo przez zaufane CA. 3. Ochrona danych (DLP) • Blokowanie urządzeń USB, dysków, kart pamięci, Bluetooth, Wi-Fi itp. • Monitorowanie operacji plikowych na nośnikach i dyskach lokalnych. • Obsługa urządzeń zewnętrznych jako „zaufanych" lub „niezaufanych". • Integracja z Windows Defender, Windows Firewall, BitLocker (w tym zdalne szyfrowanie dysków i odczyt kluczy odzyskiwania).

	• Monitorowanie TPM i antywirusów firm trzecich.
Monitoring infrastruktury	Moduł dotyczący monitorowania infrastruktury musi umożliwiać monitorowanie zasobów Sieciowych spełniając następujące minimalne wymagania: A. Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). B. Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci. C. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. D. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. E. Serwerów pocztowych: • program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, • program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, • program powinien mieć możliwość wykonywania operacji testowych, • program powinien mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa. F. Monitorowanie serwerów WWW i adresów URL. G. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. H. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP). I. Obsługa komunikatów syslog i pułapek SNMP. J. Monitoring routerów i przełączników wg: • zmian stanu interfejsów sieciowych, • ruchu sieciowego, • podłączonych stacji roboczych, • ruchu generowanego przez podłączone stacje robocze. K. Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego: • obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
Inwentaryzacja zasobów i licencji	Moduł musi gromadzić automatycznie szczegółowe dane o sprzęcie i oprogramowaniu spełniając następujące minimalne wymagania: A. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart B. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. C. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. D. Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP E. Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. F. Możliwość odczytania numeru seryjnego (klucze licencyjne). G. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. H. Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników,

	harmonogramie zadań.
Monitoring aktywności użytkowników	Moduł musi pozwalać na kontrolę aktywności użytkowników spełniając następujące minimalne wymagania: A. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. B. Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. C. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). D. Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). E. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. F. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. G. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. H. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. I. Wyświetlanie statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. J. Wyświetlanie statystyki aktywności grupy i jej członków widoczne dla menedżera grupy K. Grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. L. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. M. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). N. Przypisywanie kategorii aplikacjom i stronom internetowym, możliwość stworzenia predefiniowanej listy kategorii z możliwością edycji. O. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.
Obsługa zgłoszeń i zdalna pomoc	Moduł musi pozwalać na obsługę zgłoszeń problemów technicznych i zdalną pomoc Zapewniając następujące minimalne wymagania: A. W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. B. Pobieranie listy użytkowników z usługi katalogowej, C. Przypisywanie pracowników helpdesk do kategorii zgłoszeń. D. Procesowanie zgłoszeń użytkowników z wiadomości e-mail.

	E. Dołączanie załączników do zgłoszeń. F. Zrzuty ekranowe (podgląd pulpitu). G. Dystrybucję oprogramowania przez Agentów. H. Dystrybucję oraz uruchamianie plików za pomocą Agentów. I. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. J. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń. K. Planowanie nieobecności pracowników helpdesk. L. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA). M. Generowanie raportów obsługi helpdesk. N. Zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu). O. Możliwość użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. P. Oprogramowanie powinno posiadać komunikator. Q. Oprogramowanie powinno posiadać bazę zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
Ochrona przed wyciekiem danych	Moduł musi zapewniać ochronę danych i kontrolę urządzeń zapewniając następujące minimalne wymagania: A. Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. B. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. C. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. D. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. E. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków zewnętrznych - urządzenia nieautoryzowane. F. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. G. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. H. Możliwość usuwania z listy znanych urządzeń tych nośników
Licencja	Licencja wieczysta na co najmniej 20 stacji roboczych. Wsparcie serwisowe producenta musi obowiązywać do 31.12.2026 r.
Ilość	1 szt.

6. Wdrożenie SoftHSM (IT/OT)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Wdrożenie SoftHSM (IT/OT)
Wymagania ogólne	Zamawiający oczekuje instalacji, konfiguracji oraz uruchomienia programowego modułu bezpieczeństwa kryptograficznego HSM, przeznaczonego do bezpiecznego przechowywania kluczy kryptograficznych oraz realizacji operacji

	kryptograficznych w środowisku Zamawiającego. Rozwiązanie musi zostać wdrożone jako komponent wspierający obsługę infrastruktury klucza publicznego, podpisu elektronicznego, szyfrowania danych lub integracji z systemami wymagającymi interfejsu PKCS#11.
Wymagania dotyczące wdrożenia	W ramach wdrożenia przedmiotu zamówienia Zamawiający wymaga: 1. Przygotowania środowiska systemowego, 2. Instalacji oprogramowania, 3. Utworzenia oraz inicjalizacji repozytoriów kluczy 4. Konfiguracji mechanizmów dostępu i uprawnień administracyjnych, 5. Wygenerowania lub zaimportowanie kluczy kryptograficznych 6. Przeprowadzenia testów działania, integralności konfiguracji i komunikacji z systemami zależnymi. 7. Opracowania dokumentacji powdrożeniowej zawierającej: • Opis architektury rozwiązania, • Parametry konfiguracji, • Procedury administracyjne, • Procedury odtworzeniowe, • Rekomendacje eksploatacyjne.
Ilość	1 szt.

7. Wdrożenie infrastruktury klucza publicznego (IT/OT)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Wdrożenie infrastruktury klucza publicznego (IT/OT)
Wymagania ogólne	Zamawiający wymaga dostawy, instalacji, konfiguracji oraz uruchomienia infrastruktury klucza publicznego (PKI) w środowisku Microsoft CA Zamawiającego przeznaczonej do realizacji usług związanych z wydawaniem, zarządzaniem, publikacją, odnawianiem oraz unieważnianiem certyfikatów cyfrowych. Wdrożone rozwiązanie będzie stanowiło centralny element systemu zaufania dla usług uwierzytelniania, podpisu elektronicznego, szyfrowania danych oraz zabezpieczenia komunikacji w systemach teleinformatycznych Zamawiającego. Zakres prac: 1. Przygotowanie architektury rozwiązania. 2. Instalacja i konfiguracja urzędów certyfikacji 3. Uruchomienie usług publikacji list unieważnionych certyfikatów oraz punktów dystrybucji informacji o statusie certyfikatów. 4. Konfiguracje szablonów certyfikatów, polityk wydawania i odnawiania certyfikatów. 5. Integracja z usługami katalogowymi, systemami operacyjnymi, urządzeniami sieciowym oraz wskazanymi aplikacjami korzystającymi z mechanizmów kryptograficznych. 6. Przygotowanie polityk bezpieczeństwa. 7. Konfiguracja mechanizmów zarządzania cyklem życia certyfikatów. 8. Wdrożenie procedur administracyjnych i odtworzeniowych. 9. Przeprowadzenie testów funkcjonalnych i eksploatacyjnych potwierdzających poprawność działania całego środowiska. 10. Przygotowanie dokumentacji powdrożeniowej.
Ilość	1 szt.

8. Urządzenie NGFW do Siedziby Głównej (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie NGFW do Siedziby Głównej (IT/OT)
Wymagania ogólne	Zamawiający wymaga dostarczenia, uruchomienia i konfiguracji sprzętowego urządzenia bezpieczeństwa sieciowego realizującego funkcje ochrony sieci informatycznej siedziby głównej Zamawiającego.
Obsługa sieci	1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
Intrusion Prevention System (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą

	zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (Traffic Shapping)	1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie. 2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania). 3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. 4. Skaner antywirusowy ma pochodzić od europejskiego producenta. 5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 6. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej

	konfiguracji urządzenia. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site to- site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a) IPSec VPN, b) SSL VPN. 3. SSL VPN ma działać w trybie tunelu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. W ramach licencji dostępny jest klient SSLVPN pod systemy: Windows, Linux, macOS objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM. 8. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 9. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. 10. Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec w standardzie ML-KEM.
Filtr dostępu do stron WWW	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. 3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu. 4. Administrator ma mieć możliwość dodawania własnych kategorii URL. 5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: 6. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 7. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 8. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 9. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 10. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 11. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
Uwierzytelnianie	1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a) lokalną bazę użytkowników (wewnętrzny LDAP), b) zewnętrzną bazę użytkowników (zewnętrzny LDAP), c) usługę katalogową Microsoft Active Directory. d) Microsoft Entra ID, opartej na protokole OpenID Connect. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

	3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal) który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a) SSL, b) Radius, c) Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. 10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
Administracja łączami do internetu (ISP)	1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a) równoważenie względem adresu źródłowego, b) równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (Trasowanie)	1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

Administracja urządzeniem	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a) manualnego eksportu do pliku w dowolnym momencie czasu, b) automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie,raz w tygodniu, raz w miesiącu 18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

	2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzeniaraportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6. Urządzenie ma posiadać usługę DNS Proxy. 7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9. Urządzenie musi mieć możliwość wykorzystania REST API. 10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. 11. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
Gwarancja i serwis	Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
Parametry sprzętowe	1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 3. Liczba portów Ethernet 2,5Gbps – min. 8. 4. Liczba portów światłowodowych 1Gbps – min. 1. 5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.

	6. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. 7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 6Gbps. 8. Przepustowość typu Threat Prevention – minimum 740Mbps. 9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 3Gbps. 10. Liczba tuneli VPN IPSec – minimum 300. 11. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300. 12. Obsługa interfejsów 802.11q (VLAN) – minimum 393. 13. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 39 000 nowych sesji/sekundę. 14. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive 15. Urządzenie nie ma limitu na liczbę użytkowników. 16. Liczba reguł filtrowania – minimum 8 192. 17. Liczba tras statycznego routingu – minimum 512. 18. Liczba tras dynamicznego routingu – minimum 10 000. 19. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 20. Urządzenie musi być wyposażone w moduł TPM.
Ilość	1 szt.

9. Serwer do stworzenia infrastruktury HA (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Serwer do stworzenia infrastruktury HA (IT/OT)
Obudowa	• Obudowa Rack o wysokości max 2U • Obudowa wyposażona w ramkę przednią
Płyta główna	• Płyta główna z możliwością zainstalowania minimum jednego procesora. • Możliwość obsługi procesorów minimum 32 rdzeniowych • Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do min. 1,5TB pamięci RAM.
Procesor	• Zainstalowany minimum jeden procesor maksymalnie 16-rdzeniowy, min. 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie min. 42900 punktów w teście cpubenchmark, dostępnym na stronie https://www.cpubenchmark.net/. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	• Min. 128GB DDR5 RDIMM 4800MT/s,
Dyski twarde	• Zainstalowane min. dwa dyski SSD o pojemności min. 480GB (2x480GB) z możliwością konfiguracji RAID 1. • Zainstalowane min. sześć dysków SAS o pojemności min. 2,4TB
Gniazda PCIe	• Min. Trzy sloty PCIe
Interfejsy sieciowe/FC/SAS	• Zainstalowane min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT
Wbudowane porty	• Min. 4 porty USB w tym min: ○ 2 port USB 3.0 z tyłu obudowy, ○ 1 port USB 3.0 z przodu obudowy • Min. 1 port VGA

Video	• Zintegrowana karta graficzna z min. 16MB pamięci osiągająca rozdzielczość 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 700W klasy Platinum
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, oraz min. 20 szt. licencji dostępowych do zasobów serwera dla użytkownika. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym minimum 6 wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: A. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, B. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, C. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, D. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, E. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, F. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, G. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), H. Wbudowane wsparcie instalacji i pracy na wolumenach, które: I. Pozwalają na zamianę rozmiaru w czasie pracy systemu, I. Umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów I. Umożliwiają kompresie „w locie” dla wybranych plików i/lub folderów, V. Umożliwiają zdefiniowanie list kontroli dostępu (ACL), I. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, J. Wbudowane szyfrowanie dysków, K. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, L. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, M. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, N. Graficzny interfejs użytkownika, O. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, P. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),

	Q. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, R. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, S. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC I. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: • Podłączenie SSO do domeny w trybie offline- bez dostępnego połączenia sieciowego z domeną, • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika- na przykład typu certyfikatu użytego do logowania, • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, I. Zdalna dystrybucja oprogramowania na stacje robocze, V. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające: • Dystrybucję certyfikatów poprzez http, • Konsolidację CA dla wielu lasów domeny, • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, • Szyfrowanie plików i folderów, • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), • Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, • Serwis udostępniania stron WWW, • Wsparcie dla protokołu IP w wersji 6 (IPv6) I. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • Obsługi ramek typu jumbo frames dla maszyn wirtualnych, • Obsługi 4-KB sektorów dysków, • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • Możliwość wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być poszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, • Możliwość kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), T. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane

	przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, U. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), V. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, W. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, X. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF
Bezpieczeństwo	• Możliwość wyłączenia w BIOS funkcji natychmiastowe wyłączenie serwera za pomocą przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Opcjonalny czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155 lub równoważne. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika ○ możliwość podmontowania zdalnych wirtualnych napędów ○ wirtualną konsolę z dostępem do myszy, klawiatury ○ wsparcie dla IPv6 ○ wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ integracja z Active Directory ○ możliwość obsługi przez ośmiu administratorów jednocześnie ○ Wsparcie dla automatycznej rejestracji DNS ○ wsparcie dla LLDP ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość podłączenia lokalnego poprzez złącze RS-232. ○ Monitorowanie zużycia dysków SSD ○ możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych Możliwość rozszerzenia funkcjonalności karty o:

	○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych. ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera.

Certyfikaty	• Producent serwera musi posiadać normę ISO-9001, ISO-14001 lub równoważne. • Serwer musi posiadać deklaracja CE lub równoważną.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Gwarancja i wymagania dodatkowe	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 12 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych następującymi kanałami: telefonicznie i przez Internet. • Autoryzowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający wymaga dołączenia do oferty oświadczenia od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać autoryzacje producenta urządzenia. • Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie: ○ realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; ○ firma serwisująca posiada autoryzacje producenta oferowanego serwera;
Ilość	1 szt.

10. Urządzenie przeznaczone do stworzenia repozytorium kopii zapasowych (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie przeznaczone do stworzenia repozytorium kopii zapasowych (IT/OT)
Specyfikacja sprzętowa	Procesor: Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.2 GHz Procesor liczba rdzeni: Nie mniej niż 4 Pamięć RAM: Nie mniej niż 4GB DDR4 Pamieć RAM liczba slotów: Minimum 2 sloty

	Pamięć RAM - możliwość rozszerzenia: Nie mniej niż do 64GB Pamięć Flash: Nie mniej niż 5 GB Liczba zatok na dyski twarde: Minimum 8 Obsugiwane dyski twarde: 3.5" oraz 2.5" SATA oraz 2.5" SATA SSD Pojemność dysków twardych możliwych do stosowania: do 20TB Obsługa dysków M2 PCIe: Tak, minimum 2 porty Gen3x1 Możliwość podłączenia modułu rozszerzającego: Tak, minimum 9, może wymagać dodatkowej karty rozszerzeń Porty LAN 2,5 GbE: Minimum 2 RJ-45 Diody LED: Minimum Status, LAN, HDD Porty USB 3.2 Gen2 (10 Gb/s): Minimum 2 Typ C i 2 Typ A Port PCiE: Tak, minimum 1 Gen3x8 Przyciski: Reset, Zasilanie Typ obudowy: RACK, maksymalnie 2U Dopuszczalna temperatura pracy: od 0 do 40°C Wilgotność względna podczas pracy: 5-95% R.H. Zasilanie: Zasilacz min. 2x250 W, 100-240 V
Specyfikacja oprogramowania	Agregacja łączy Tak Obsługiwane systemy plików: • Dyski wewnętrzne: EXT4 • Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ Szyfrowanie wolumenów Tak, min AES 256 Szyfrowanie dysków zewnętrznych Tak Zarządzanie dyskami • Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, • Obsługa Hot Spare per grupa RAID oraz global hot spare • Rozszerzanie pojemności Online RAID • Migracja poziomów Online RAID • HDD S.M.A.R.T. • Skanowanie uszkodzonych bloków (pliku) • Przywracanie macierzy RAID • Obsługa map bitowych • Pula pamięci masowej • Obsługa migawek • Obsługa replikacji migawek Wbudowana obsługa iSCSI • Multi-LUNs na Target • Obsługa LUN Mapping & Masking • Obsługa SPC-3 Persistent Reservation • Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN Zarządzanie prawami dostępu • Ograniczenie dostępnej pojemności dysku dla użytkownika • Importowanie listy użytkowników • Zarządzanie kontami użytkowników • Zarządzanie grupą użytkowników • Zarządzanie współdzieleniem w sieci • Tworzenie użytkowników za pomocą makr • Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL Obsługa Windows AD

	• Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web • Funkcja serwera LDAP Funkcje backup • Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, Współpraca z zewnętrznymi dostawcami usług chmury Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box Darmowe aplikacje na urządzenia mobilne • Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki • Dostępne na systemy iOS oraz Android Minimum obsługiwane serwery • Serwer plików • Serwer FTP • Serwer WEB • Serwer kopii zapasowych • Serwer multimediów UPnP • Serwer pobierania (Bittorrent / HTTP / FTP) • Serwer Monitoringu VPN • VPN client / VPN server. Obsługa PPTP, OpenVPN Administracja systemu • Połączenia HTTP/HTTPS • Powiadamianie przez e-mail (uwierzytelnianie SMTP) • Powiadamianie przez SMS • Ustawienia inteligentnego chłodzenia • DDNS oraz zdalny dostęp w chmurze • SNMP (v2 & v3) • Obsługa UPS z zarządzaniem SNMP (USB) • Obsługa sieciowej jednostki UPS • Monitor zasobów • Kosz sieciowy dla CIFS/SMB oraz AFP • Monitor zasobów systemu w czasie rzeczywistym • Rejestr zdarzeń • Całkowity rejestr systemowy (poziom pliku) • Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line • Aktualizacja oprogramowania • Możliwość aktualizacji oprogramowania • Ustawienia: Back up, przywracania, resetowania systemu Wirtualizacja • Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5

	Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. Konteneryzacja • Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker Zabezpieczenia • Filtracja IP • Ochrona dostępu do sieci z automatycznym blokowaniem • Połączenie HTTPS • FTP z SSL/TLS (Explicit) • Obsługa SFTP (tylko admin) • Szyfrowanie AES 256-bit • Szyfrowana zdalna replikacja (Rsync poprzez SSH) • Import certyfikatu SSL • Powiadomienia o zdarzeniach za pośrednictwem Email i SMS Możliwość instalacji dodatkowego oprogramowania • Tak, sklep z aplikacjami; możliwość instalacji z paczek
Zainstalowane dyski	Minimum 4 dyski spełniające poniższe wymagania: • Pojemność minimum 8TB każdy • Typ dysku: HDD • Interfejs dysku: SATA III
Gwarancja	Minimum 12 miesięcy gwarancji producenta.
Ilość	1 szt.

11. Przełącznik dostępowy do Siedziby Głównej (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Przełącznik
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz.
Porty	Minimum: • 4 porty SFP/SFP+ lub SFP28 min. 10 Gb/s • 24 porty 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at • 1 port konsolowy RJ45 lub równoważny • 1 port typu USB do transferu plików • Budżet mocy PoE min. 380 W
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity minimum 128 Gbps Forwarding rate minimum 95 Mpps Pamięć flash minimum 128 MB Pamięć RAM minimum 512 MB
Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (IEEE 802.3ad) Obsługa minimum 8 grup LACP Obsługa ramek Ethernet typu Jumbo minimum 9k
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego Obsługa minimum 512 wpisów routingu dynamicznego
Inne Funkcjonalności	Obsługa list kontroli dostępu opartych o adresy MAC i IP Ochrona DoS

	Storm Control Broadcast/Multicast/Unknown Unicast DHCP Snooping DHCP Relay DHCP Server IGMP Snooping BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p QoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority Narzędzia diagnostyczne PING, TRACEROUTE, ICMP TFTP, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej
Zgodność z protokołami	IEEE 802.1AB LLDP ANSI/TIA-1057 LLDP-MED IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1p Class of Service (CoS) IEEE 802.1Q VLAN Tagging IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1X Port Based Network Access Control IEEE 802.2 Logical Link Control IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet (100BASE-TX) IEEE 802.3ab Gigabit Ethernet (1000BASE-T) IEEE 802.3x Flow Control IEEE 802.3ad Link Aggregation Control Protocol (LACP) RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP lub równoważny mechanizm synchronizacji czasu RFC 2132 DHCP Options i BOOTP Vendor Extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta, wraz z bezpłatnym dostępem do aktualizacji oprogramowania.
Ilość	1 szt.

12. Przełącznik CORE do Siedziby Głównej (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Przełącznik

Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 2U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz.
Porty	Minimum: • 4 porty SFP/SFP+ lub SFP28 min. 10 Gb/s • 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at • 1 port konsolowy RJ45 lub równoważny • 1 port typu USB do transferu plików • Budżet mocy PoE min. 400 W
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity minimum 176 Gbps Forwarding rate minimum 120 Mpps Pamięć flash minimum 128 MB Pamięć RAM minimum 512 MB
Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (IEEE 802.3ad) Obsługa minimum 8 grup LACP Obsługa ramek Ethernet typu Jumbo minimum 9k
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego Obsługa minimum 512 wpisów routingu dynamicznego
Inne Funkcjonalności	Obsługa list kontroli dostępu opartych o adresy MAC i IP Ochrona DoS Storm Control Broadcast/Multicast/Unknown Unicast DHCP Snooping DHCP Relay DHCP Server IGMP Snooping BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p QoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority Narzędzia diagnostyczne PING, TRACEROUTE, ICMP TFTP, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej
Zgodność z protokołami	IEEE 802.1AB LLDP ANSI/TIA-1057 LLDP-MED IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1p Class of Service (CoS) IEEE 802.1Q VLAN Tagging IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1X Port Based Network Access Control IEEE 802.2 Logical Link Control IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet (100BASE-TX) IEEE 802.3ab Gigabit Ethernet (1000BASE-T)

	IEEE 802.3x Flow Control IEEE 802.3ad Link Aggregation Control Protocol (LACP) RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP lub równoważny mechanizm synchronizacji czasu RFC 2132 DHCP Options i BOOTP Vendor Extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta, wraz z bezpłatnym dostępem do aktualizacji oprogramowania.
Ilość	1 szt.

13. Klucze U2F dla głównego administratora (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Klucze U2F dla głównego administratora
Wymagania ogólne	Przedmiotem zamówienia jest dostawa sprzętowego klucza uwierzytelniającego obsługującego technologię NFC (Near Field Communication) ze złączem USB-A.
Wymagania funkcjonalne	1. Urządzenie musi umożliwiać: • Uwierzytelnianie FIDO2/WebAuthn • Uwierzytelnianie FIDO U2F. 2. Urządzenie musi wspierać logowanie: • Bezhasłowe • Dwuskładnikowe (2FA) • Wieloskładnikowe (MFA) 3. Klucz musi działać bez konieczności instalacji dodatkowego oprogramowania na obsługiwanych systemach. 4. Uwierzytelnianie użytkownika musi odbywać się poprzez: • Fizyczne dotknięcie klucza przy wykorzystaniu USB-A, • Zbliżenie klucza do urządzenia z obsługą NFC.
Wymagania dotyczące interfejsów komunikacyjnych	1. Klucz musi posiadać: • Złącze USB-A zgodne ze standardem USB 2.0. • Interfejs NFC umożliwiający komunikację między urządzeniami mobilnymi.
Wymagania dotyczące kompatybilności	1. Urządzenie musi być kompatybilne z następującymi systemami operacyjnymi: • Microsoft Windows, • macOS, • Linux, • ChromeOS. 2. Urządzenie musi umożliwiać współpracę z usługami wspierającymi standardy FIDO2/U2F, m.in.: • Google, • Microsoft (w tym Outlook, OneDrive, Office),
Wymagania	1. Klucz musi wykorzystywać mechanizmy kryptograficzne oparte o klucze

bezpieczeństwa	publiczne zgodnie z FIDO2. 2. Urządzenie musi być: • odporne na phishing oraz przejęcie konta, • odporne na ataki typu Man-in-the-Middle (MiTM). 3. Urządzenie nie może przechowywać danych osobowych użytkownika; dane logowania muszą być przechowywane w sposób bezpieczny i nieodwracalny. 4. Klucz musi być odporny na: • działanie wody, • zgniecenia, • uszkodzenia mechaniczne. 5. Urządzenie nie może zawierać baterii ani elementów ruchomych.
Certyfikaty i zgodność	Urządzenie musi być zgodne ze standardami FIDO Alliance: • FIDO2 • FIDO U2F
Gwarancja	Minimum 24 miesiące gwarancji..
Ilość	2 szt.

14. Szafa rack na urządzenia (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Szafa RACK dla urządzeń (IT/OT)
Wymagania ogólne	Zamawiający wymaga dostarczenia szafy instalacyjnej typu RACK 19” o wysokości minimalnej 15U przeznaczonej do montażu urządzeń teleinformatycznych.
Wymagania techniczne	Typ: szafa instalacyjna RACK Standard montażowy: 19 cali Wysokość użytkowa: maksymalnie 16U Wymiary zewnętrzne (szerokość x głębokość): minimalnie 600 x 450mm Konstrukcja: metalowa Obciążenie: minimalne 60kg. Drzwi przednie: szklane Panel wentylacyjny: wymagane otwory wentylacyjne min. 120mm
Wymagane wyposażenie	Komplet śrub 2x półka RACK 19 cali (szerokość x głębokość): maksymalnie 600 x 350mm
Zgodność ze standardami	ANSI/EIA RS-310D lub równoważne, IEC297-2 lub równoważne, DIN41494; PART1 & PART7 lub równoważne, ETSI lub równoważne
Gwarancja	Minimum 36 miesięcy gwarancji producenta
Ilość	1 szt.

15. Access Point do Siedziby Głównej (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Access Point do Siedziby Głównej (IT/OT)
	• Zintegrowana dwupolaryzacyjna antena dookólna

	• Dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach oraz obsługujące następujące standardy: a) 2.4 GHz 802.11 b/g/n/ax b) 5 GHz 802.11 a/n/ac Wave 2/ax • Zgodność z normami IEEE 802.11 a/b/g/n/ac/ax • Moc transmisyjna: minimum 20dBm dla 2.4 GHz oraz 20dBm dla 5GHz • Zysk anteny: minimum 4dBi dla 2.4 GHz oraz 5dBi dla 5 GHz • Obudowa zapewniająca prawidłową pracę w poniższych warunkach: a) Temperatura: 0º C do +40º C b) Wilgotność: do 90% • Maksymalny pobór mocy: 26W • Zasilanie: PoE+ • Minimum 1 x port Rj45 (10/100/1000 Mbps) • Interfejs radiowy wspierający funkcję 2x2:2 MU-MIMO • Jednoczesne rozgłaszanie minimum 16 SSID łącznie na obu modułach radiowych • Minimum 8 profili WLAN per radio • Minimalna deklarowana liczba klientów: 120 • Możliwość kształtowania wiązki (beamforming) • Tryb zarządzania – bez kontrolera, z wykorzystaniem kontrolera chmurowego lub kontrolera na maszynie wirtualnej • Obsługa maksymalnej szybkość transmisji danych: a) 2,4 GHz – 573,5Mbps b) 5 GHz – 2402Mbps • Wsparcie dla poniższych metod uwierzytelniania: WPA2-Enterprise, WPA3-Enterprise, IEEE 802.1X • Możliwość ustawienia harmonogramu włączania i wyłączania sieci WLAN z podziałem na dni, tygodnie lub godziny. • Możliwość ustawienia limitu danych dla klienta z wykorzystaniem bitrate, czasu sesji, przepustowości konfigurowane per SSID
Gwarancja	Gwarancja producenta min. 60 miesięcy.
Ilość	5 szt.

16. Audyt wraz z testami bezpieczeństwa infrastruktury sieciowej/sprzętowej (IT/OT)

Nazwa	Minimalne wymagania dla audytu
Typ	Audyt wraz z testami bezpieczeństwa infrastruktury sieciowej/sprzętowej (IT/OT)
Wymagana ogólne	Audyt bezpieczeństwa informacji wraz z raportem poaudytowym. Audyt bezpieczeństwa informacji wraz z raportem podsumowującym, zgodnie z normą ISO 27001
I Audyt techniczny	1. Zakres Audytu technicznego, musi skupiać się na weryfikacji infrastruktury IT, w tym zabezpieczeń fizycznych, komputerów, usług, dostępu do sieci, systemów kopii zapasowych oraz uruchomionych usług bezpieczeństwa. 2. Musi zostać przeprowadzany na określonej infrastrukturze IT, zgodnie z dobrymi praktykami cyberbezpieczeństwa.

	3. Audyt musi zakończyć się raportem zawierającym minimum przegląd infrastruktury, ocenę procedur aktualizacji, kontroli dostępu oraz zalecenia dotyczące zauważonych podatności. 4. Pełny Audyt Techniczny_swoim zakresem obejmuje tylko weryfikację infrastruktury IT, określonej w ramach umowy ze stroną audytowaną. Ma być przeprowadzany w oparciu o dobre praktyki cyberbezpieczeństwa oraz wiedzę wyznaczonych audytorów inżynierów. Może być realizowany stacjonarnie i zdalnie. Audyt powinien obejmować: wizję lokalną w siedzibie Zamawiającego, a jeśli to zasadne, również wizje zdalne, w zakresie w jakim jest to możliwe do wykonania; sprawdzenie wszystkich wskazanych przez Zamawiającego elementów infrastruktur IT; weryfikację, jak zabezpieczone pod względem zachowania poufności, dostępności, integralności przechowywane są przetwarzane dane; Zamawiającego nie wymaga przeglądu i analizy dokumentacji oraz weryfikacji stanu zastanego na podstawie wewnętrznej dokumentacji W ramach audytu technicznego podlegać powinna.: ocena zabezpieczeń fizycznych (dostęp do serwerowni, sprzętu IT) ocena zabezpieczeń komputerów (poziomy uprawnień, wykorzystywane oprogramowanie) ocena zabezpieczeń usług (serwery, oprogramowanie) ocena zabezpieczenia dostępu do infrastruktury sieciowej (aktywne urządzenia sieciowe) ocena konfiguracji systemów kopii zapasowych ocena uruchomionych usług zapewniających bezpieczeństwoEfektem końcowym powinien być raport z audytu technicznego, który zawiera w sobie m. in.: przegląd fizyczny pomieszczeń serwerowni przegląd urządzeń serwerowych zainstalowanych w serwerowni przegląd urządzeń serwerowych i sieciowych zainstalowanych poza serwerownią Wynik technicznej weryfikacji infrastruktury sieciowej wraz z oceną zastosowanych reguł adresacji, segmentacji w warstwie drugiej modelu TCP/IP oraz reguł bezpieczeństwa zarządzania ruchem sieciowym. Ocenę procedury przeprowadzania aktualizacji systemów wraz z weryfikacją na przykładach w środowisku. ocenę technicznej realizacji kontroli dostępu do urządzeń oraz procedur uwierzytelniania i autoryzacji użytkowników. Ocenę wdrożonych mechanizmów zarządzania stacjami roboczymi - przydział polityk, zainstalowane oprogramowanie itp. Ocenę stanu i wykorzystanego potencjału istniejących systemów bezpieczeństwa oraz ich dedykowanych mechanizmów. Raport zawiera również zalecenia z zakresu zauważonych podatności.
II Audyt bezpieczeństwa informacji	1. Przeprowadzenie audytu bezpieczeństwa informacji ma na celu ocenę rzeczywistego poziomu bezpieczeństwa informacji oraz stosowanych zabezpieczeń w oparciu o dobre praktyki cyberbezpieczeństwa określone w normie PN/EN ISO/IEC ISO 27001:2023. 2. Wykonawca zobowiązany jest w razie zaistnienia potrzeby do uczestnictwa w spotkaniach zorganizowanych z Zamawiającym w celu omówienia postępu prac i analizowanej dokumentacji. Zamawiający dopuszcza spotkania w postaci zdalnej. 3. Zakres prac audytowych ma obejmować zarówno analizę dokumentacji dostarczonej przez Zamawiającego, jak i infrastruktury informatycznej oraz

	fizycznej. Powinna zostać przeprowadzona weryfikacja infrastruktury budynków pod kątem zapewniania kontroli dostępu i bezpieczeństwa informacji oraz zapewnienia ciągłości działania. Weryfikacji powinny podlegać również serwerownie/ punkty dystrybucyjne, wyposażenie IT oraz systemów pomocniczych dla IT: systemy CCTV, klimatyzacja, wentylacja, systemy p. poż, czujniki środowiskowe, zasilanie awaryjne (UPS/agregat) znajdujące się w głównej serwerowni. Sprawdzony powinen zostać także aktywny sprzęt sieciowy, środowisko serwerowe oraz pamięci masowych, w tym ich wsparcie serwisowe, gwarancje producenta i ich konfiguracja. Ponadto powinno zostać zweryfikowane : • usługi katalogowe (Active Directory) w ramach jej podstawowej konfiguracji bezpieczeństwa - zgodności z istniejącymi politykami bezpieczeństwa organizacji. • usługi sieciowe takie jak DNS, DHCP, RADIUS, syslog . • katalogi udostępnione • centrum certyfikacji lokalnego środowiska PKI • oprogramowanie antywirusowe, XDR, kopii bezpieczeństwa, 3.1. Audyt musi zostać przeprowadzony w odniesieniu do normy dotyczącej procedur i zasad bezpieczeństwa, tj. ISO/IEC 27001:2023 w oparciu o próbki audytowe odnoszące się do wymagań normy. 3.2. Audyt zostanie przeprowadzony w odniesieniu do normy dotyczącej procedur i zasad bezpieczeństwa, tj. ISO/IEC 27001:2023 w oparciu o próbki audytowe odnoszące się do wymagań normy w zakresie: 4. Zarządzanie zasobami ludzkimi, w tym budowanie kompetencji i uświadamianie 5. Zarządzanie łańcuchem dostaw 6. Zarządzanie bezpieczeństwem fizycznym 7. Zarządzanie kontrolą dostępu IT 8. Zarządzanie bezpieczeństwem sieci i ochroną przed złośliwym oprogramowaniem 9. Zarządzanie kopiami bezpieczeństwa i redundancją środków wspomagających przetwarzanie informacji 10. Zarządzanie zdarzeniami i incydentami dla bezpieczeństwa informacji 11. Zarządzanie pracą zdalną i pracą poza obszarami bezpiecznymi 12. Zarządzanie usuwaniem informacji 13. Zarządzanie ryzykiem w bezpieczeństwie informacji 14. Zarządzanie ciągłością działania 15. Zarządzanie aktywami informacyjnymi i wspierającymi 16. Zarządzanie organizacją w aspekcie bezpieczeństwa informacji 17. Zarządzanie projektami w zakresie bezpieczeństwa informacji 18. Zarządzanie kodami źródłowymi 19. Zarządzanie oprogramowaniem i zarządzanie zmianami 20. Zarządzanie kryptografią 21. Zarządzanie bezpieczeństwem informacji podczas badań, audytów i testów Audyt bezpieczeństwa musi składać się z 3 etapów: Etap I Przegląd i analiza dokumentów. Zamawiający dostarczy w terminie 14 dni roboczych od dnia podpisania umowy posiadaną przez siebie dokumentację związaną z systemem zarządzania bezpieczeństwem informacji, czyli m.in.: • Wewnętrzne procedury bezpieczeństwa informacji (np. procedura kontroli dostępu, nadawania uprawnień etc.)

	• Politykę ochrony danych osobowych • Osobowy schemat organizacyjny • Zakres systemu zarządzania bezpieczeństwem informacji • Wykaz procesów (w tym procesy podzlecane) • Wykaz lokalizacji wraz z zakresem działania • Inne dokumenty poruszające tematykę bezpieczeństwa informacji, które stanowią podstawę do stwierdzenia zgodności z wymaganiami normy. Etap II Audyt lokalny zrealizowany w ustalonym przez obie strony terminie (Zamawiającego i Wykonawcę) w siedzibie Zamawiającego w dni robocze w godzinach 08:00-16:00. Przeprowadzenie audytu jest możliwe w weekendy lub w innych godzinach pracy, ustalonych wcześniej przez obie strony. Metodyka audytu Audyt musi być przeprowadzony przy pomocy analizy dokumentacji, list kontrolnych, obserwacji pracy wykonywanej w siedzibie Zamawiającego, próbek i dowodów (zbieranych subiektywnie), rozmów z wyznaczonymi osobami audytowanymi (zgodnie z planem) oraz wybranymi pracownikami w ramach wizji lokalnej w siedzibie Zamawiającego. Etap III – raport z audytu i zalecenia – efekt przeprowadzonych prac Raport poaudytowy – w dokumencie tym musi znaleźć się podsumowanie przebiegu etapu I i etapu II audytu bezpieczeństwa informacji zawierający wytyczne z zakresu zabezpieczeń i dobrych praktyk zaproponowanych na podstawie doświadczenia i wiedzy audytorów w oparciu o normę. Szczegółowa zawartość raportu poaudytowego musi zawierać: • Zapisy zawierające wnioski, zalecenia i rekomendacje, które mają na celu zapoznanie Zamawiającego z istniejącymi niezgodnościami lub podatnościami wpływającymi na poziom ryzyka zaistnienia zagrożeń wraz ze wskazaniem zalecanych działań naprawczych. • Obserwacje audytowe • Wyniki testów i ich interpretacje • Listę wykrytych podatności opatrzonych komentarzem audytora
Ilość	1 szt.

17. Montaż i konfiguracja urządzeń UTM, przełączników aktualizacja do najnowszej wersji oprogramowania, wydzielenie vlanów, separacja sieci Wdrożenie oprogramowania XDR (IT/OT)

Nazwa	Minimalne wymagania dla usługi
Typ	Montaż i konfiguracja urządzeń UTM, przełączników aktualizacja do najnowszej wersji oprogramowania, wydzielenie vlanów, separacja sieci Wdrożenie oprogramowania XDR (IT/OT)
Wymagania ogólne	Zamawiający wymaga, aby Wykonawca dokonał wdrożenia proponowanych rozwiązań według poniższych wymagań minimalnych: 1. Wdrożenie oprogramowania antywirusowego XDR wskazanego w Opisie Przedmiotu Zamówienia : • Instalacja serwera konsoli EDR na maszynie wskazanej przez Zamawiającego, • Wstępna konfiguracja, • Przygotowanie wstępnych, domyślnych polityk,

	• Wdrożenie agenta EDR, • Sprawdzenie poprawności działania serwera konsoli EDR, • Przegląd detekcji zgromadzonych w konsoli, • Wspólna analiza i optymalizacja, • Wspólne tworzenie wykluczeń, Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania. 2. Wdrożenie i konfiguracja urządzeń UTM wskazanych w Opisie Przedmiotu Zamówienia wraz z wydzieleniem vlanów • Wstępna konfiguracja urządzeń UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Wdrożenia system RADIUS w ramach posiadanego ekosystemu • Stworzenie interfejsów (VLAN) oraz ich adresacja • Konfiguracja podstawowych polityk firewall • Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) • Integracja z Active Directory + Agent SSO • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP 3. Wdrożenie i konfiguracja przełączników wskazanych w Opisie Przedmiotu Zamówienia • Demontaż starych przełączników • Instalacja w szafach rack zamawiającego nowych przełączników • Aktualizacja oprogramowania przełączników do najnowszej dostępnej wersji, wydzielenie vlanów, separacja sieci • Podstawowa konfiguracja przełączników tj. interfejsy do zarządzania, konto administracyjne. Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska.
Ilość	1 szt.

18. UPS dla serwerowni w Siedzibie Głównej (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	UPS dla serwerowni w Siedzibie Głównej (IT/OT)
Wymagania minimalne	Moc wyjściowa (pozorna / czynna): minimum 3000 VA minimum 2700 W Topologia: (on-line double conversion) Typ obudowy: Rack max 2U Chłodzenie: Wymuszone, wewnętrzne wentylatory
Wejście	Napięcie znamionowe (wartość skuteczna): 230 V AC

	Zakres napięcia wejściowego (wartości skuteczne) 185 ÷ 280 V AC Częstotliwość znamionowa napięcia wejściowego: 50/60 Hz Zakres częstotliwości 40 ÷ 70 Hz Progi przełączania: sieć – UPS: 120 ÷ 276 V AC
Wyjście	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa: 220 ÷ 240 V AC ± 2 % Kształt napięcia wyjściowego : Sinusoidalny Częstotliwość znamionowa napięcia wyjściowego: 50 Hz Filtracja napięcia wyjściowego: pełna filtracja ciągła (całkowita izolacja od zakłóceń sieciowych) Progi przełączania: UPS – sieć: 176 ÷ 276 V AC ± 2 % Czas przełączenia na pracę rezerwową 0 ms Czas powrotu na pracę sieciową: 0 ms Przeciążalność > 105% - 12 s
Akumulatory i czasy podtrzymania	Akumulatory wewnętrzne: minimum 6x 12 V / 9 Ah Czas podtrzymania (100 % / 80 % / 50 % Pmax): minimum 2 / 4 / 8 min
Zabezpieczenia	Zabezpieczenie wejściowe • Przeciwzwarciowe – Bezpiecznik automatyczny • 16 A / 250 V AC • Przeciwprzepięciowe Zabezpieczenie wyjściowe: Elektroniczne – przeciwzwarciowe i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe
Wyposażenie i funkcje dodatkowe	Przyłącza wyjściowe (liczba i typ gniazd) • minimum 6 x IEC320 C13 (10 A) • minimum 1 x IEC C19 (16 A) Sygnalizacja minimum: Akustyczno – optyczna; graficzny wyświetlacz LCD Interfejsy komunikacyjne minimum: USB Wsporniki do montażu w szafie RACK • Oprogramowanie tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na stanowiskach komputerowych w sieci - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów. możliwość edycji nazw urządzeń na liście monitorowanych UPSów Możliwość aktualizacji firmware w UPS przez użytkownika
Certyfikaty	Producent oferowanego sprzętu musi posiadać ISO 9001:2015 lub równoważne dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania
Gwarancja	minimum 24 miesięcy na elektronikę i 24 miesiące na akumulatory; Serwis musi być realizowany przez autoryzowany serwis producenta. Zamawiający wymaga, aby serwis realizowany był w systemie door to door
Ilość	1 szt.

19. UPS dla serwerowni (NAS) (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	UPS dla serwerowni (NAS) (IT/OT)
Wymagania	Moc wyjściowa (pozorna / czynna): minimum 1200 VA minimum 600 W

minimalne	Topologia: Line-Interactive (z układem AVR) Typ obudowy: Tower
Wejście	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wejściowego (wartości skuteczne) 185 ÷ 280 V AC Częstotliwość znamionowa napięcia wejściowego: 50/60 Hz Zakres częstotliwości 45 ÷ 60 Hz Progi przełączania: sieć – UPS: 140 ÷ 270 V AC
Wyjście	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa: 200 ÷ 230 V AC Kształt napięcia wyjściowego: aproksymacja sinusoidy Częstotliwość znamionowa napięcia wyjściowego: 50/60 Hz Filtracja napięcia wyjściowego: Podstawowa filtracja zakłóceń sieciowych i tłumienie impulsów Progi przełączania: UPS – sieć: 160 ÷ 270 V AC Czas przełączenia na pracę rezerwową 10 ms Czas powrotu na pracę sieciową: 5 ms
Akumulatory i czasy podtrzymania	Akumulatory wewnętrzne: minimum 1x 12 V / 9 Ah Czas podtrzymania (80 % / 50 % Pmax): minimum 1 / 4 min
Zabezpieczenia	Zabezpieczenie wejściowe • Przeciwzwarciowe – Bezpiecznik automatyczny • 5 A / 250 V AC • Przeciwprzepięciowe Zabezpieczenie wyjściowe: Elektroniczne – przeciwzwarciowe i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe
Wyposażenie i funkcje dodatkowe	Przyłącza wyjściowe (liczba i typ gniazd) • minimum 4 x Schuko Sygnalizacja minimum: Akustyczno – optyczna; dioda LED Interfejsy komunikacyjne minimum: USB • Oprogramowanie tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności.
Certyfikaty	Producent oferowanego sprzętu musi posiadać ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania
Gwarancja	minimum 24 miesięcy na elektronikę i 24 miesiące na akumulatory; Serwis musi być realizowany przez autoryzowany serwis producenta. Zamawiający wymaga, aby serwis realizowany był w systemie door to door
Ilość	1 szt.

20. UPS dla stacji w Siedzibie Głównej - druga szafa (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	UPS dla stacji w Siedzibie Głównej - druga szafa (IT/OT)
Wymagania minimalne	Moc wyjściowa (pozorna / czynna): minimum 1200 VA minimum 600 W Topologia: Line-Interactive (z układem AVR) Typ obudowy: Tower
Wejście	Napięcie znamionowe (wartość skuteczna): 230 V AC

	Zakres napięcia wejściowego (wartości skuteczne) 185 ÷ 280 V AC Częstotliwość znamionowa napięcia wejściowego: 50/60 Hz Zakres częstotliwości 45 ÷ 60 Hz Progi przełączania: sieć – UPS: 140 ÷ 270 V AC
Wyjście	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa: 200 ÷ 230 V AC Kształt napięcia wyjściowego: aproksymacja sinusoidy Częstotliwość znamionowa napięcia wyjściowego: 50/60 Hz Filtracja napięcia wyjściowego: Podstawowa filtracja zakłóceń sieciowych i tłumienie impulsów Progi przełączania: UPS – sieć: 160 ÷ 270 V AC Czas przełączenia na pracę rezerwową 10 ms Czas powrotu na pracę sieciową: 5 ms
Akumulatory i czasy podtrzymania	Akumulatory wewnętrzne: minimum 1x 12 V / 9 Ah Czas podtrzymania (80 % / 50 % Pmax): minimum 1 / 4 min
Zabezpieczenia	Zabezpieczenie wejściowe • Przeciwzwarciowe – Bezpiecznik automatyczny • 5 A / 250 V AC • Przeciwprzepięciowe Zabezpieczenie wyjściowe: Elektroniczne – przeciwzwarciowe i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe
Wyposażenie i funkcje dodatkowe	Przyłącza wyjściowe (liczba i typ gniazd) • minimum 4 x Schuko Sygnalizacja minimum: Akustyczno – optyczna; dioda LED Interfejsy komunikacyjne minimum: USB • Oprogramowanie tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności.
Certyfikaty	Producent oferowanego sprzętu musi posiadać ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania
Gwarancja	minimum 24 miesięcy na elektronikę i 24 miesiące na akumulatory; Serwis musi być realizowany przez autoryzowany serwis producenta. Zamawiający wymaga, aby serwis realizowany był w systemie door to door
Ilość	1 szt.

21. Agregat z przyczepą transportową (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Agregat z przyczepą transportową (IT/OT)
Wymagania ogólne	Spalinowy zespół prądotwórczy wyposażony w, czterosuwowy silnik wysokoprężny w układzie rzędowym, prądnicę, wyłącznik główny, ramę nośną urządzenia, w której zainstalowany będzie zbiornik paliwa.
Konfiguracja	Agregat prądotwórczy wyposażony w silnik wysokoprężny połączony z prądnicą – zespół prądotwórczy zamontowany do ramy za pośrednictwem metalowo gumowych tłumików drgań typu silent block. Rama wykonana ze stalowych profili malowanych.

	Agregat prądotwórczy w obudowie dźwiękochłonnej redukującej emisję hałasu na zewnątrz oraz stanowiącym zabezpieczenie przed wpływem działania czynników atmosferycznych oraz osób trzecich.
Minimalna moc brutto PRP silnika spalinowego [kW]	37 kW
Minimalna znamionowa moc elektryczna PRP agregatu [kVA] / [kW]	40 kVA / 32 kW
Minimalna moc awaryjna elektryczna ESP agregatu [kVA] / [kW]	45 kVA / 36 kW
Maksymalna pojemność skokowa silnika [L]	2,3 L
Układ dolotowy	Wyposażony w filtry powietrza wlotowego
Układ chłodzenia	Układ chłodzenia silnika wyposażony w naramową chłodnicę wentylatorową z wentylatorem napędzanym bezpośrednio z wału korbowego silnika poprzez przekładnie pasową, bez wykorzystania napędu elektrycznego. Chłodnica naramowa wyposażona w układ orurowania, mocowania wentylatora. Układ chłodzenia wyposażony w postojowy układ podgrzewania bloku silnika podczas przestoju urządzenia w trybie standby. Układ podgrzewania wyposażony w grzałkę elektryczną.
Układ rozruchowy	Wyposażony w akumulator rozruchowy oraz rozrusznik. Podczas pracy urządzenia akumulator ładowany poprzez alternator, podczas przestoju możliwe jest ładowanie ładowarką zintegrowaną z agregatem prądotwórczym.
Prądnica	Minimum 3 fazowa
Typ prądnicy	Samowzbudna, jednołożyskowa, 1500 RPM
Napięcie nominalne, częstotliwość	Minimum 3 x 400V , 50Hz
Klasa izolacji prądnicy	Min. H
Stopień ochrony IP prądnicy	Min. IP23
Dokładność regulacji	Min. 1.0 %
Regulator obrotów silnika	Elektroniczny
Zgodność z normami	ISO8528 lub równoważne
Technologia wykonania obudowy	Wykonana ze stali poddana procesowi galwanizacji a następnie malowana proszkowo w kolorystyce RAL
Konstrukcja agregatu	Agregat umieszczony w obudowie odpornej na warunki atmosferyczne, przystosowanej pracy w warunkach zewnętrznych.
Maksymalna masa netto agregatu w bez paliwa [kg]	850kg
Podramowy zbiornik paliwa – pojemność [L]	Gwarantujący minimum 12 h pracy ciągłej agregatu przy 100% obciążeniu mocą znamionową
Drzwi	Umożliwiające pełną obsługę serwisową, eksploatacyjną z zewnątrz, jedne z

	drzwiczek wyposażone w okno rewizyjne do podglądu parametrów pracy agregatu, bez konieczności ich otwierania. Drzwi wyposażone w zawiasy, klamki z zamkami blokującymi przed dostępem osób trzecich
Zatrzymanie awaryjne	Przycisk awaryjny zainstalowany na zewnątrz kontenera do awaryjnego zatrzymania zespołu prądotwórczego
Wyposażenie agregatu/kontenera	Grzałka cieczy chłodzącej, Ładowarka baterii akumulatorów rozruchowych
Certyfikaty producenta	Producent agregatu prądotwórczego musi posiadać certyfikat ISO 9001 oraz AQAP 2110 lub równoważny
Wymagania właściwości sterownika zespołu prądotwórczego	- monitorowanie pracy agregatu, - oparty o technologie mikroprocesorową, - umożliwia automatyczną kontrolę i sterowanie aparatami sieci i agregatu w panelu przełączania źródła SZR, - kontrola parametrów mech. Silnika i elektrycznych generatora, - sygnalizacja alarmów przy użyciu diod LED i na wyświetlaczu LCD, - rejestracja zdarzeń, - prosta obsługa za pomocą przycisków sterujących i wyświetlacza LCD z czytelnym menu.
Sposób odbioru mocy z zespołu prądotwórczego	Każdy agregat wyposażony w gniazda zewnętrzne, minimum: 3 x 16A Schuko 1 x 16A 5P 1 x 32A 5P Oraz listwę odbioru mocy
Awaryjne uruchomienie zespołu prądotwórczego	Zespół prądotwórczy musi umożliwiać jego rozruch i pracę z pominięciem sterownika agregatu (w przypadku jego awarii i demontażu) z zachowaniem ochrony silnika od wysokiej temperatury cieczy i niskiego ciśnienia oleju.
Dostawa i odbiory	Dostawa na obiekt, kompletnych i gotowych do pracy urządzeń do lokalizacji wskazanej przez Zamawiającego
Wymagania dodatkowe	Agregaty prądotwórcze muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż w 2026 roku na terenie Unii Europejskiej - Zamawiający wymaga aby serwis gwarancyjny przeprowadzony był przez pracownika dostawcy posiadającego autoryzację producenta oferowanych agregatów prądotwórczych, - Spełnienie punktów określających parametry przedmiotowego dokumentu wynikać powinno z przedłożonych kart katalogowych lub innych dokumentów producenta. Agregat w obudowie technologicznej dostarczony będzie na przyczepie platformowej umożliwiające tylko i wyłącznie manewrowanie po terenie wewnętrznym. Agregat prądotwórczy nie będzie przeznaczony do zastosowań mobilnych po drogach publicznych. Przyczepa jest elementem zamówienia.
Gwarancja na agregat prądotwórczy wraz z wyposażeniem dodatkowym	Minimum 24 miesiące z limitem 1000 motogodzin. Producent w czasie trwania gwarancji wykona gwarancyjne przeglądy okresowe na własny koszt. Na potwierdzenie wymogu, wymagane jest dołączenie do oferty oświadczenia producenta, że: producent agregata w czasie trwania gwarancji wykona gwarancyjne przeglądy okresowe na własny koszt producenta agregatu potwierdza minimum 24 miesiące gwarancji z limitem 1000 motogodzin.

Ilość	2 szt.

III. OBSZAR TECHNICZNY OT

1. Przełącznik do lokalizacji zdalnej (OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Przełącznik
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 2U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz.
Porty	Minimum: • 4 porty SFP/SFP+ lub SFP28 min. 10 Gb/s • 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at • 1 port konsolowy RJ45 lub równoważny • 1 port typu USB do transferu plików • Budżet mocy PoE min. 400 W
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity minimum 176 Gbps Forwarding rate minimum 120 Mpps Pamięć flash minimum 128 MB Pamięć RAM minimum 512 MB
Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (IEEE 802.3ad) Obsługa minimum 8 grup LACP Obsługa ramek Ethernet typu Jumbo minimum 9k
Funkcjonalność warstwy III	Obsługa minimum 64 wpisów routingu statycznego Obsługa minimum 512 wpisów routingu dynamicznego
Inne Funkcjonalności	Obsługa list kontroli dostępu opartych o adresy MAC i IP Ochrona DoS Storm Control Broadcast/Multicast/Unknown Unicast DHCP Snooping DHCP Relay DHCP Server IGMP Snooping BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p QoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority Narzędzia diagnostyczne PING, TRACEROUTE, ICMP TFTP, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej
Zgodność z	IEEE 802.1AB LLDP

protokołami	ANSI/TIA-1057 LLDP-MED IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1p Class of Service (CoS) IEEE 802.1Q VLAN Tagging IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1X Port Based Network Access Control IEEE 802.2 Logical Link Control IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet (100BASE-TX) IEEE 802.3ab Gigabit Ethernet (1000BASE-T) IEEE 802.3x Flow Control IEEE 802.3ad Link Aggregation Control Protocol (LACP) RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP lub równoważny mechanizm synchronizacji czasu RFC 2132 DHCP Options i BOOTP Vendor Extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta, wraz z bezpłatnym dostępem do aktualizacji oprogramowania.
Ilość	2 szt.

2. Sprzętowe sondy monitorujące w ramach systemu klasy IDS dla OT, umożliwiające bezpieczne oraz pasywne zbieranie kopii ruchu sieciowego (OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Sprzętowe sondy monitorujące w ramach systemu klasy IDS dla OT, umożliwiające bezpieczne oraz pasywne zbieranie kopii ruchu sieciowego (OT)
Przeznaczenie i funkcja	Zamawiający wymaga dostarczenia minimum trzech (3) sprzętowych sond monitorujących pracujących w ramach dostarczanego systemu klasy IDS dla środowisk przemysłowych OT umożliwiających bezpieczne, pasywne i bezinwazyjne zbieranie kopii ruchu sieciowego w sieciach IT/OT. Sondy muszą zapewniać: • Ciągłe, pasywne monitorowanie komunikacji sieciowej, • Zbieranie i analizę ruchu sieciowego, • Budowę modelu komunikacji w sieci przemysłowej, • Wykrywanie zagrożeń, incydentów oraz anomalii w komunikacji. Licencja systemu klasy IDS musi być wieczysta i współpracować z nielimitowaną liczbą monitorowanych urządzeń. Gwarancja producenta wraz ze wsparciem technicznym- minimum 24 miesiące. .
Wymagania	Sondy monitorujące muszą:

ogólne i bezpieczeństwo pracy	• działać w sposób w pełni pasywny (100% passive), • nie generować żadnego ruchu w monitorowanej sieci, • nie wpływać na dostępność, opóźnienia ani niezawodność komunikacji, • analizować ruch wyłącznie na podstawie jego kopii, • zapewniać pełną transparentność dla urządzeń OT (PLC, HMI, SCADA itd.), • być częścią jednego, spójnego rozwiązania IDS (ten sam producent).
Metody pozyskiwania ruchu sieciowego	Sondy muszą obsługiwać następujące tryby pracy: • odbiór ruchu poprzez porty SPAN / mirror przełączników, • pracę w trybie pass-through / in-line (bez ingerencji w transmisję), • analizę kopii ruchu bez aktywnego udziału w komunikacji.
Interfejsy monitorujące i sprzętowe	Interfejsy Ethernet: • min. 1 port RJ45 10/100 Mbps do monitoring ruchu. Port musi: ○ działać wyłącznie w trybie odbioru (RX only) ○ nie posiadać funkcji transmisji (brak TX) ○ nie identyfikować się w sieci (brak widocznego MAC) • Interfejsy przemysłowe: Sonda musi wspierać pasywny monitoring komunikacji dla minimum: ○ RS485 ○ RS422 ○ RS232 ○ CAN
Funkcjonalność analityczna sond	Sondy muszą umożliwiać: • przekazywanie danych do systemu IDS w czasie rzeczywistym • selektywne przekazywanie ruchu (filtracja): ○ po adresach IP ○ po urządzeniach ○ po protokołach • eksport i przekazywanie danych w formacie: ○ IPFIX • współpracę z analizą: ○ DPI (deep packet inspection) ○ ML/AI (po stronie systemu IDS) • obsługę przechwytywania pakietów (PCAP – przez system IDS).
Wymagania bezpieczeństwa	Sondy muszą zapewniać: • szyfrowanie danych przechowywanych lokalnie: ○ minimum AES 128-bit, • zabezpieczenie przed manipulacją: ○ automatyczne kasowanie danych przy próbie nieautoryzowanego dostępu do pamięci FLASH, • ochronę fizyczną: ○ detekcję otwarcia obudowy, ○ generowanie alarmu w systemie IDS, • szyfrowaną komunikację z centralnym systemem IDS
Wymagania instalacyjne	Sondy muszą: • umożliwiać montaż w warunkach przemysłowych: ○ instalacja na szynie DIN • być przystosowane do pracy ciągłej (24/7/365), • być odporne na przerwy w zasilaniu i warunki środowiskowe, • umożliwiać instalację bez przerywania pracy sieci, • nie powodować zakłóceń transmisji podczas wdrożenia.
Zasilanie i niezawodność	Sondy muszą: • być zasilane napięciem 24 VDC,

	• posiadać podtrzymanie zasilania (battery backup): ○ minimum 30 minut pracy, • zapewniać bezpieczne zapisanie danych w przypadku zaniku zasilania.
Zarządzanie i integracja	Sondy muszą umożliwiać: • zdalne zarządzanie i konfigurację z poziomu systemu IDS, • aktualizację oprogramowania i firmware, • monitorowanie stanu urządzenia, • konfigurację parametrów pracy, • komunikację z systemem IDS w sposób szyfrowany, • pracę w sieci z: ○ DHCP ○ statyczną konfiguracją IP.
Integracja z systemem IDS	Sondy muszą: • współpracować z centralnym systemem IDS w zakresie: ○ analizy ruchu, ○ detekcji zagrożeń, ○ mapowania sieci OT, • umożliwiać: ○ analizę protokołów przemysłowych, ○ wykrywanie anomalii, ○ identyfikację incydentów, • przekazywać dane do systemu w czasie rzeczywistym, • umożliwiać centralne aktualizacje i zarządzanie.
Wymagania dodatkowe	Sondy muszą zapewniać: • brak ograniczeń funkcjonalnych wynikających z architektury sprzętowej, • możliwość pracy w środowiskach o wysokim poziomie bezpieczeństwa, • kompatybilność z architekturą przemysłową Zamawiającego, • możliwość rozbudowy systemu przez dodanie kolejnych sond.
Serwis i gwarancja	Dostarczana licencja systemu IDS musi być licencją wieczystą dla nielimitowanej liczby monitorowanych urządzeń. Gwarancja producenta wraz ze wsparciem technicznym- minimum 24 miesiące. Serwis producenta systemu IDS musi obejmować: • Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim. • Dostęp do nowych wersji systemu IDS. • Dostęp do aktualizacji i poprawek systemu IDS. • Dostęp do aktualizacji oprogramowania sond sprzętowych. • Wymianę uszkodzonych sond sprzętowych w razie awarii. • Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS. • Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji. • Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
Wdrożenie	Wdrożenie musi być przeprowadzone przez Wykonawcę w zakresie minimum: • Instalacja, oraz konfiguracja systemu IDS w środowisku serwerowym wskazanym przez Zamawiającego, • Instalacja sond sprzętowych w miejscach wskazanych przez Zamawiającego. • Pełna konfiguracja i wdrożenie systemu u Zamawiającego • Przekazanie Zamawiającemu wszelkich haseł użytych w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.

	• Przeprowadzenie testów sprawdzających prawidłowość instalacji, konfiguracji i działania systemu. • Szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Szkolenie może być przeprowadzone zdalnie. • Przygotowanie dokumentacji powykonawczej opisującej wszystkie prace, sposób konfiguracji poszczególnych urządzeń oraz całego wdrożenia.
Ilość	1 szt. (1 system składający się z minimum 3 sprzętowych sond monitorujących)

3. UPS dla lokalizacji zdalnej (OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	UPS dla lokalizacji zdalnej (OT)
Wymagania minimalne	Moc wyjściowa (pozorna / czynna): minimum 1000 VA minimum 900 W Topologia: (on-line double conversion) Typ obudowy: Rack max 2U Chłodzenie: Wymuszone, wewnętrzne wentylatory
Wejście	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wejściowego (wartości skuteczne) 185 ÷ 280 V AC Częstotliwość znamionowa napięcia wejściowego: 50/60 Hz Zakres częstotliwości 40 ÷ 70 Hz Progi przełączania: sieć – UPS: 120 ÷ 276 V AC
Wyjście	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa: 220 ÷ 240 V AC ± 2 % Kształt napięcia wyjściowego : Sinusoidalny Częstotliwość znamionowa napięcia wyjściowego: 50 Hz Filtracja napięcia wyjściowego: pełna filtracja ciągła (całkowita izolacja od zakłóceń sieciowych) Czas przełączenia na pracę rezerwową 0 ms Czas powrotu na pracę sieciową: 0 ms Przeciążalność > 105% - 15 s
Akumulatory i czasy podtrzymania	Akumulatory wewnętrzne: minimum 3x 12 V / 7 Ah Czas podtrzymania (100 % / 80 % / 50 % Pmax): minimum 2 / 4 / 6 min
Zabezpieczenia	Zabezpieczenie wejściowe • Przeciwzwarciowe – Bezpiecznik automatyczny • 10 A / 250 V AC • Przeciwprzepięciowe Zabezpieczenie wyjściowe: Elektroniczne – przeciwzwarciowe i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe
Wyposażenie i funkcje dodatkowe	Przyłącza wyjściowe (liczba i typ gniazd) • minimum 4 x IEC320 C13 (10 A) Sygnalizacja minimum: Akustyczno – optyczna; graficzny wyświetlacz LCD Interfejsy komunikacyjne minimum: USB Wsporniki do montażu w szafie RACK • Oprogramowanie tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na stanowiskach komputerowych w sieci - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów. możliwość edycji nazw urządzeń na liście

	monitorowanych UPSów Możliwość aktualizacji firmware w UPS przez użytkownika
Certyfikaty	Producent oferowanego sprzętu musi posiadać ISO 9001:2015 lub równoważne dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania
Gwarancja	minimum 24 miesięcy na elektronikę i 24 miesiące na akumulatory; Serwis musi być realizowany przez autoryzowany serwis producenta. Zamawiający wymaga, aby serwis realizowany był w systemie door to door
Ilość	1 szt.

4. Dedykowany dysk do przeprowadzania kopii zapasowych w środowiskach OT, które nie mają dostępu do sieci lokalnej/internetu (OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Dedykowany dysk do przeprowadzania kopii zapasowych w środowiskach OT, które nie mają dostępu do sieci lokalnej/internetu (OT)
Wymagania ogólne	Przedmiotem zamówienia jest dostawa mobilnego urządzenia przeznaczonego do zabezpieczania i przywracania systemów IT oraz technologii operacyjnych ICS/OT. Urządzenie musi zapewniać pełną funkcjonalność w trybie offline, bez wymaganego dostępu do sieci LAN lub Internetu. Zastosowanie rozwiązania musi umożliwiać realizację procedur Business Continuity i Disaster Recovery
Parametry techniczne i pojemność	Urządzenie musi posiadać wbudowaną pamięć o pojemności min. 1 TB na składowanie kopii zapasowych. Urządzenie musi posiadać metalową obudowę w celu zapewnienia bezpieczeństwa kopii zapasowych w warunkach środowisk pracy przemysłowej. Urządzenie musi posiadać port USB-A lub USB-C w celu podłączenia do zabezpieczanego urządzenia. Nie dopuszcza się podłączania urządzenia za pomocą innych portów (np. RJ45).
Funkcjonalność backupu	Rozwiązanie musi pozwalać na wykonywanie kopii obrazu dysku (image-level backup) urządzenia, na którym system został uruchomiony. Rozwiązanie musi pozwalać na wykonywanie kopii pełnej oraz przyrostowej. Rozwiązanie musi pozwalać na wykorzystanie kompresji i deduplikacji. Rozwiązanie powinno zapewniać pełną kontrolę użytkownika nad częstotliwością wykonywania kopii. Rozwiązanie musi umożliwiać backup systemów operacyjnych z rodziny Windows (w tym Windows Embedded) oraz Linux. Rozwiązanie musi pozwalać na zabezpiezanie środowisk odizolowanych poprzez wykonywanie kopii offline. Oznacza to, iż rozwiązanie musi pozwalać na wykonywanie backupu urządzeń, które nie są podpięte do sieci. Możliwość tworzenia bootowalnego nośnika bezpośrednio z urządzenia w celu przywracania systemów. Rozwiązanie musi posiadać zdolność do przenoszenia kopii danych pomiędzy różnymi magazynami.
Funkcje odzyskiwania danych	Możliwość przywracania kopii obrazu dysku na oryginalne urządzenie lub na sprzęt o innej konfiguracji sprzętowej. Rozwiązanie musi wspierać wersjonowanie. Każda wersja backupu możliwa do odtworzenia musi być odzwierciedleniem każdego wykonania kopii zapasowej.
Integracja i zgodność	Urządzenie musi funkcjonować jako niezależna jednostka, niewymagająca zewnętrznej infrastruktury serwerowej do przeprowadzenia procesu backupu lub przywracania oraz niewymagająca nadrzędnego oprogramowania backupowego,

	do którego jest podłączona.
Gwarancja	Minimum 36 miesięcy gwarancji producenta
Ilość	1 szt.

5. Urządzenie UTM dla lokalizacji zdalnych z ochroną protokołów przemysłowych (OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenie UTM dla lokalizacji zdalnych z ochroną protokołów przemysłowych (OT)
Wymagania ogólne	Zamawiający wymaga dostarczenia urządzenia bezpieczeństwa sieciowego klasy UTM/NGFW przeznaczonego w szczególności do monitorowania, kontroli i ochrony komunikacji w sieciach przemysłowych (OT) oraz zabezpieczenia instalacji technologicznych i punktów infrastruktury krytycznej. Rozwiązanie musi umożliwiać inspekcję i analizę ruchu sieciowego z wykorzystaniem protokołów przemysłowych stosowanych w systemach automatyki, sterowania oraz monitoringu procesów technologicznych. Urządzenie powinno pełnić rolę zapory sieciowej oraz punktu kontroli ruchu pomiędzy strefami sieciowymi (IT/OT), umożliwiając bezpieczną separację, monitorowanie i kontrolę połączeń. Rozwiązanie musi być przystosowane do pracy ciągłej w środowisku przemysłowym oraz umożliwiać centralne zarządzanie i analizę zdarzeń bezpieczeństwa.
Obsługa sieci	1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w

	oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
Intrusion Prevention System (IPS)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz 6. JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 7. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 8. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 9. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 10. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). 11. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (Traffic Shapping)	1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Wirtualne sieci prywatne (VPN)	1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny– lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. IPSec VPN, b. SSL VPN. 3. SSL VPN ma działać w trybie tunelu. 4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

	6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 7. W ramach licencji dostępny jest klient SSLVPN pod systemy: Windows, Linux, macOS objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM. 8. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 9. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based. 10. Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec w standardzie ML-KEM.
Uwierzytelnianie	1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. d. Microsoft Entra ID, opartej na protokole OpenID Connect. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. 10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
Administracja łączami do internetu (ISP)	1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane

	osobno dla każdego z łączy do Internetu. 4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (Trasowanie)	1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
Administracja urządzeniem	1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer

	(syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie,raz w tygodniu, raz w miesiącu 18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzeniaraportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 5. Urządzenie ma posiadać usługę DNS Proxy. 6. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 7. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 8. Urządzenie musi mieć możliwość wykorzystania REST API. 9. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego

	(firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
Gwarancja i serwis	Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu dla wszystkich funkcji bezpieczeństwa. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
Parametry sprzętowe	1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD 3. Liczba portów Ethernet 2,5Gbps – min. 4. 4. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 5. Przepustowość Firewall (1518 bajtów UDP) – minimum 8,5Gbps 6. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. 7. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1,8Gbps. 8. Liczba tuneli VPN IPSec – minimum 200 9. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 200 10. Obsługa interfejsów 802.11q (VLAN) – minimum 137. 11. Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 25 000 nowych sesji/sekundę. 12. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive 13. Urządzenie nie ma limitu na liczbę użytkowników. 14. Liczba reguł filtrowania – minimum 1024. 15. Liczba tras statycznego routingu – minimum 512. 16. Liczba tras dynamicznego routingu – minimum 10 000. 17. Urządzenie musi posiadać pasywny system chłodzenia. 18. Urządzenie ma być przystosowane do pracy w temperaturach od -20 stopni Celsjusza do +60 stopni Celsjusza przy wilgotności od 0% do 95% (bez kondensacji) 19. Średni czas bezawaryjnej pracy (MTBF) w temperaturze +25 stopni Celsjusza musi być nie mniejszy niż 50 lat. 20. Urządzenie musi być przystosowane do montażu na szynie DIN zgodnej ze standardem EN 50022. 21. Urządzenie musi być wyposażone w moduł TPM. 22. Urządzenie musi dawać możliwość podłączenia zasilania bezpośrednio z linii produkcyjnej prądem stałym 12-48VDC 3-0.75A. 23. Urządzenie musi być wyposażone w zasilacz umożliwiający podłączenie do sieci 100-240V 60-50Hz 1.2A.
Ilość	1 szt.

IV. OBSZAR KOMPETENCYJNY

1. Szkolenie dotyczące cyberbezpieczeństwa i cyberhigieny dla pracowników, działu IT oraz kadry zarządzającej poprzedzone symulowanymi atakiem phishingowym (IT/OT)

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenie dotyczące cyberbezpieczeństwa i cyberhigieny dla pracowników, działu IT oraz kadry zarządzającej poprzedzone symulowanymi atakiem phishingowym

	(IT/OT)
	W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do przeprowadzenia testów phishingowych (TP) wg poniższego zakresu minimalnego: 1. Zamawiający wymaga ustalenia scenariusza w zakresie minimum: • Opracowania i zatwierdzenia z Zamawiającym szczegółowego scenariusza ataku socjotechnicznego. • Wyboru metod i narzędzi do jego realizacji. • Szczegóły kampanii, w tym scenariusze socjotechniczne oraz harmonogram realizacji, muszą zostać ustalone i zatwierdzone przez Zamawiającego co najmniej 14 dni przed planowanym rozpoczęciem kampanii. 2. Zamawiający wymaga przeprowadzenia przygotowań ataku w zakresie minimum: • Projektowanie minimum jednego szablonu • Przygotowanie minimum jednej fałszywej domeny i konfiguracja hostingu. • Listy odbiorców • Finalizacja listy docelowych odbiorców w oparciu o informacje uzyskane od Zamawiającego. 3. Zamawiający wymaga przeprowadzenia startu realizacji ataku w zakresie minimum: • Rozpoczęcie kampanii phishingowej: kampania musi zostać przeprowadzona w ciągu minimum 3 dni, rozpoczynając się od wysyłki mailowej do wybranych odbiorców. 4. Zamawiający wymaga kontynuacji kampanii i monitorowania w zakresie minimum: • Dostosowania harmonogramu wysyłki do ustaleń przeprowadzonych z Zamawiającym na etapie ustalania scenariusza. • Czas trwania kampanii: minimum 3 dni robocze, liczba dni zostaje dostosowana w oparciu o ustalenia z Zamawiającym podczas pierwszego etapu jakim jest ustalenie scenariusza. • Kampania powinna być realizowana etapami, z wysyłkami dokonywanymi w określonych partiach i godzinach, aby zapewnić maksymalną skuteczność. • Bieżące śledzenie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami • Analizy efektywności i w razie potrzeby, wprowadzanie zmian w strategii kampanii. 5. Zamawiający wymaga przeprowadzenia zakończenia kampanii i przygotowanie raportu w zakresie minimum: • Zebrania i dokonania pierwszej analizy zebranych danych na temat interakcji i reakcji na przeprowadzone działania. • Przygotowania raportu końcowego dotyczącego skuteczności kampanii, zawierającego wszystkie zebrane dane, w zakresie minimum: ○ opis wykorzystanych i skonfigurowanych domen ○ opis szablonów oraz opis celu jaki stanowił podczas realizacji kampanii ○ opis niebezpieczeństw związanych z dalszymi krokami prawdziwego ataku ○ statystyki kampanii phishingowej, w tym: liczby wysłanych, otwartych maili, liczby kliknięć w link, liczby osób, które podały swoje dane podsumowanie oraz rekomendacje.
Szkolenie cyberbezpieczeństwa	Szkolenie musi zostać przeprowadzone w maksymalnie dwóch grupach liczących maksymalnie 20 osób. Szkolenie dla każdej grupy musi trwać minimum 1 godzinę. Wymagane jest, aby szkolenie przeprowadzone było, w formie online. Szkolenie musi być zrealizowane w formie vouchera z możliwością zrealizowania

	w wybranym przez Zamawiającego terminie do 31.12.2026 Szkolenie musi obejmować w zakresie minimum: • Czym jest Cyberbezpieczeństwo? • Wycieki informacji – mechanizmy i skutki. • Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze. • Psychomanipulacja w sieci – zasady i zastosowania. • Sfałszowane komunikaty i strony – identyfikacja zagrożeń. • Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing) • Archiwizacja internetowa – cyfrowy ślad nie znika. • Mechanizmy śledzenia w sieci – rola i funkcja cookies. • Niebezpieczeństwa ze strony nieautoryzowanego sprzętu. • Ataki siłowe na hasła – jak nie dać się złamać. • Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing). • Świadomość pracowników – kultura bezpieczeństwa w organizacji.
Wymagania dodatkowe	Zamawiający wymaga, aby szkolenia dedykowane dla pracowników jednostki zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.
Ilość	1 szt.

2. Szkolenie dla działu IT z rozwiązania NGFW, ITSM, XDR, System operacyjny serwera (IT/OT)

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenie dla działu IT z rozwiązania NGFW, ITSM, XDR, System operacyjny serwera (IT/OT)
Szkolenie NGFW	Wykonawca zapewni szkolenie (minimum 2 dni) dla Administratora Zamawiającego (1 osoba) dotyczące rozwiązania wskazanego w Opisie Przedmiotu Zamówienia . Urządzenie NGFW do Siedziby Głównej (IT/OT). Zamawiający dopuszcza szkolenie w formule online. Program szkolenia musi obejmować w zakresie minimum: 1. Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego, 2. Ustawienia systemowe i uprawnienia administratorów, 3. Instalacja licencji i aktualizacja systemu, 4. Tworzenie kopii zapasowej i przywracanie konfiguracji, 5. Zbieranie logów i monitorowanie, 6. Przedstawienie kategorii zbieranych logów, 7. Typy obiektów i ich wykorzystywane 8. Obiekty sieciowe i obiekt typu „router”. 9. Konfiguracja sieci, 10. Tryby pracy urządzenia, 11. Typy interfejsów, 12. Typy routingu, 13. Translacja adresów sieciowych (NAT), 14. Translacja połączeń wychodzących 15. Translacja połączeń przychodzących, 16. Filtrowanie ruchu sieciowego (Firewall) 17. Filtrowane ruchu i koncepcji śledzenia połączeń, 18. Ochrona aplikacji,

	19. Użytkownicy i uwierzytelnianie, 20. Konfiguracja usługi katalogowej, 21. Wirtualne sieci prywatne (VPN) 22. SSL VPN. Zamawiający wymaga, aby szkolenia zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń. Szkolenie musi być zrealizowane w formie vouchera z możliwością zrealizowania w wybranym przez Zamawiającego terminie do 30.12.2026 r.
Szkolenie ITSM	Zamawiający wymaga przeprowadzenia szkolenia minimum dwudniowego (2), w formie stacjonarnej lub on-line. Platforma bezpieczeństwa łącząca oprogramowanie ITSM, monitorowania infrastruktury informatycznej, zarządzać zasobami i licencjami, ITSM, SAM, CMDB (IT/OT). Minimalny zakres tematyczny: • Najważniejsze funkcjonalności oprogramowania, • Poprawna konfiguracja oprogramowania, • Wymagania i instalacja systemu, • Sposoby aktualizacji, • Ćwiczenia praktyczne z wdrażania systemu, • Monitoring krytycznych urządzeń w organizacji, • Przeprowadzanie audytu oprogramowania i sprzętu, • Monitorowanie aktywności użytkowników, • Automatyzacja procesów obsługi zgłoszeń serwisowych, • Zarządzanie nośnikami zewnętrznymi, • Zarządzanie wskaźnikami aktywności pracowników. Dodatkowo Zamawiający wymaga aby uczestnik szkolenia otrzymał: • Materiały szkoleniowe w wersji elektronicznej • Wsparcie poszkoleniowe trenera w okresie minimum 14 dni po zakończeniu szkolenia. Zamawiający wymaga, aby szkolenia zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń. Szkolenie musi być zrealizowane w formie vouchera z możliwością zrealizowania w wybranym przez Zamawiającego terminie do 30.12.2026 r.
Szkolenie XDR	Wykonawca zapewni szkolenie (minimum 2 dni)) dla Administratora Zamawiającego (1 osoba) dotyczące rozwiązania wskazanego w Opisie Przedmiotu Zamówienia. Platforma bezpieczeństwa łącząca oprogramowanie antywirusowe, oprogramowanie MDM, oprogramowanie EDR/XDR. Zamawiający dopuszcza szkolenie online. Szkolenie powinno zostać dostarczone w formie vouchera z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do 31.12.2026. Program szkolenia musi obejmować w zakresie minimum: 1. Omówienie podstawowych pojęć związanych z Threat Huntingiem, 2. Przygotowanie playbook'a. 3. Wdrożenie serwera XDR, 4. Wdrożenie agenta XDR, 5. Omówienie konsoli XDR oraz danych które zbiera, 6. Podstawowe detekcje i reagowanie,

	7. Uruchomienie podstawowej detekcji,, 8. Weryfikacja incydentu, 9. Wykluczenia i ich tworzenie, 10. Przeprowadzenie analizy powłamaniowej, 11. Raportowanie i powiadomienia. Szkolenie musi zakończyć się autoryzowanym egzaminem producenta. Pozytywnie zdany egzamin zakończony musi być otrzymaniem certyfikatu producenta.
Szkolenie przełączniki	Wykonawca zapewni szkolenie dla Administratora Zamawiającego dotyczące sprzętu sieciowego dostarczanego w ramach grantu rozwiązania wskazanego w Opisie Przedmiotu Zamówienia. Przełącznik CORE do Siedziby Głównej (IT/OT) Minimalny zakres tematyczny szkolenia: 1. Rejestracja w systemie platformy zarządzającej 2. Wprowadzenie użytkownika do interfejsu platformy zarządzającej oraz podstawowych funkcjonalności systemu. 3. Dodawanie urządzeń do platformy zarządzającej. 4. Weryfikacja statusu urządzeń oraz podstawowe operacje związane z zarządzaniem ich dostępnością. 5. Zarządzanie oprogramowaniem przełączników w tym aktualizację firmware 6. Wykonywanie podstawowych czynności administracyjnych, w tym tworzenie kopii konfiguracji 7. Monitorowanie pracy urządzeń w zakresie dostępnych funkcjonalności systemu 8. Wprowadzenie do mechanizmów centralnego zarządzania konfiguracją przełączników 9. Tworzenie oraz zarządzanie grupami przełączników (Switch Group) 10. Przypisywanie urządzeń do grup konfiguracyjnych 11. Tworzenie oraz zarządzanie sieciami VLAN w środowisku przełączników (warstwa L2) 12. Przypisywanie VLAN do przełączników oraz grup konfiguracyjnych 13. Konfiguracja portów przełączników 14. Konfigurację oraz zarządzanie funkcjonalnością zasilania PoE (jeśli dotyczy) 15. Realizację podstawowych czynności diagnostycznych dostępnych w ramach systemu 16. Omówienie dobrych praktyk w zakresie zarządzania i utrzymania środowiska przełączników
Szkolenie z systemu operacyjnego	Wykonawca zapewni szkolenie (minimum 2h) dla Administratora Zamawiającego w środowisku Microsoft Windows Server posiadanym przez Zamawiającego, dotyczące minimum : Instalacja i konfiguracja kontrolerów domeny • Omówienie usług AD DS • Omówienie kontrolerów domeny usług AD DS • Wdrożenie kontrolera domeny • Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server Zarządzanie obiektami w AD DS • Zarządzanie kontami użytkowników • Zarządzanie grupami w usługach AD DS • Zarządzanie obiektami typu komputer w AD DS • Wdrażanie i zarządzanie OU

	Zarządzanie zaawansowaną infrastrukturą AD DS • Wprowadzenie do zaawansowanych wdrożeń AD DS • Wdrożenie rozproszonego środowiska AD DS • Konfiguracja relacji zaufania AD DS Wdrażanie i zarządzanie lokacjami i repliką AD DS • Omówienie replikacji usług AD DS • Konfigurowanie lokacji usług AD DS • Konfigurowanie i monitorowanie replikacji usług AD DS Wdrażanie zasad grupy • Wprowadzenie do zasad grupy • Wdrażanie i zarządzanie obiektami GPO (Group Policy Object) • Konfiguracja zakresu i przetwarzania obiektów GPO • Rozwiązywanie problemów z GPO Zarządzanie ustawieniami użytkowników za pomocą zasad grupy • Wdrażanie szablonów administracyjnych • Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów • Konfiguracja preferencji zasad grupowych
Wymagania dodatkowe	Zamawiający dopuszcza szkolenie online. Zamawiający wymaga, aby szkolenia dedykowane dla pracowników jednostki zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. Szkolenie musi być zrealizowane w formie vouchera z możliwością zrealizowania w wybranym przez Zamawiającego terminie do 30.12.2026 r.
Ilość	1 szt.