Załącznik numer 1 do Zapytania ofertowego
DTE / ZP12 / 2026

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 8

1. Serwer fizyczny niezbędny do zainstalowania produktu lud wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA typ 1 8

2. Serwer fizyczny niezbędny do zainstalowania produktu lud wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA typ 2 20

3. Serwery do kopii zapasowych 33

4. Network Attached Storage (NAS) – Siedziba Główna 43

5. Network Attached Storage (NAS)- pozostałe jednostki 46

6. UTM- Unified Threat Protection -do Siedziby Głównej wraz z analiza protokołów przemysłowych OT (IT/OT) typ 1 48

7. UTM- Unified Threat Protection do lokalizacji zdalnych wraz z analiza protokołow przemysłowych OT (IT/OT) typ 2 56

8. Zarządzalne urządzenia sieciowe (switch) typ 1 64

9. Zarządzalne urządzenia sieciowe (switch) typ 2 66

10. Zarządzalne urządzenia sieciowe (switch) typ 3 68

11. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa typ 1 70

12. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa typ 2 71

13. Oprogramowanie antywirusowe 71

14. Oprogramowanie do monitorowania infrastruktury informatycznej 91

15. Usługa SOC (Security Operations Center) IT/OT/ICS/IIoT 96

16. Oprogramowanie przeciwdziałające wyciekowi danych (DLP- Data Leak Prevetion) 128

17. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa 131

18. Wdrożenie usługi Active Directory wraz z wpięciem użytkowników do domeny 132

19. Fizyczny montaż serwerów wraz z aktualizacją oprogramowania, fizyczny montaż i konfiguracja urządzeń UPS 132

20. Wdrożenie oprogramowania antywirusowego, wdrożenie oprogramowania do monitorowania infrastruktury informatycznej, wdrożenie oprogramowania przeciwdziałającego wyciekowi danych, wdrożenie oprogramowania do tworzenia kopii zapasowych 133

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"

21. Centralny manager haseł w wersji On-Premise 134

22. Klucze sprzętowe U2F 141

III. OBSZAR TECHNICZNY OT 142

1. Separacja sieci IT/OT, wdrożenie urządzeń UTM, instalacja i wdrożenie przełączników sieciowych 142

2. Oprogramowanie typu NDR (Network Detection & Response) 144

IV. OBSZAR KOMPETENCYJNY 147

1. Dostęp do platformy edukacyjnej z zakresu cyberbezpieczeństwa dla pracowników w celu regularnego podnoszenia świadomości i SZBI (IT/OT) 147

2. Szkolenie dotyczące cyberbezpieczeństwa i cyberhigieny dla pracowników, działu IT oraz kadry zarządzającej 151

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"

WSTĘP

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Zakładu Usług Wodno-Ściekowych Sp. z o.o. w Słubicach 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.

I. WYMAGANIA OGÓLNE

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.

O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis: " Zainstalowany jeden procesor 8-rdzeniowy, min. 2.3Ghz klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku 20.900 w teście Average CPU Mark Multithread Rating dostępnym na stronie https://www.cpubenchmark.net/ należy rozumieć jako:

"Zainstalowany co najmniej jeden procesor, posiadający co najmniej 8 rdzeni, klasy co najmniej x86, posiadające taktowanie co najmniej 2.3GHz, umożliwiające osiągnięcie wyniku co najmniej 20 900 w teście Average CPU Mark Multithread Rating dostępnym na stronie https://www.cpubenchmark.net/".

II. OBSZAR TECHNICZNY IT

1. Serwer fizyczny niezbędny do zainstalowania produktu lud wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA typ 1

Nazwa	Minimalne wymagania dla sprzętu
Typ	Sprzęt serwerowy wraz z niezbędnym oprogramowaniem
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji maksymalnie 8 dysków 2.5” • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora • Możliwość obsługi procesorów 144 rdzeniowych • Płyta główna musi być zaprojektowana przez producenta serwera. • Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczone do instalacji pamięci • Płyta główna powinna obsługiwać do 1.5TB pamięci RAM.
Procesor	Zainstalowany min. jeden procesor min. 16-rdzeniowy, min. 3.6GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 206 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	• Minimum 128GB pamięci RAM DDR5 RDIMM 6400MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający: o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących o Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	• Zainstalowane: o Min. 4x dysk SSD SATA o pojemności min. 960GB, Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1
Gniazda PCI	• Min. Dwa sloty PCIe Gen5
Interfejsy sieciowe/FC/SAS	• Min. 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Min. Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28

Wbudowane porty	• Min. 4 porty USB w tym min: o 1 port USB 2.0 Type-C o 2 porty USB 3.1 o 1 port USB 3.0 wewnątrz obudowy • Min. 1 Port VGA z tyłu obudowy
Video	• Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200
Zasilacze	• Redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium.
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny / dodatkowe oprogramowanie	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Zamawiający wymaga dostarczenia minimum 40 szt. Licencji dostępowych do SSO użytkowników. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i minimum czterech 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,

	II. Umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów III. Umożliwiają kompresie „w locie" dla wybranych plików i/lub folderów, IV. 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 II. 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, III. Zdalna dystrybucja oprogramowania na stacje robocze, IV. 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) VI. 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

Wentylatory	• Redundantne
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • 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).
Karta zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika o możliwość podmontowania zdalnych wirtualnych napędów o wirtualną konsolę z dostępem do myszy, klawiatury o wsparcie dla IPv6 o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.

	o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer o integracja z Active Directory o możliwość obsługi przez ośmiu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej o możliwość podłączenia lokalnego poprzez złącze RS-232. o możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. o Monitorowanie zużycia dysków SSD o możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, o Automatyczne zgłaszanie alertów do centrum serwisowego producenta o Automatyczne update firmware dla wszystkich komponentów serwera o Możliwość przywrócenia poprzednich wersji firmware o Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON o Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych o Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. o Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera o Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. Możliwość rozszerzenia funkcjonalności karty o: 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. o kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania o Automatyczne odświeżanie certyfikatów SSL

	o możliwość wykorzystania tokenu do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej o możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień o możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera o możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer o możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe o monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is" do innych konsol firm trzecich o Możliwość definiowania ról administratorów

	o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o 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, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. o Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej

Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów

	▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware: o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty: o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:

	▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo: o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspieranie urządzenia: o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent: o Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności: o Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne: o Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne. • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami lub równoważne. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie

	materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.
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.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany 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 oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga dołączenia do oferty oświadczeniaod 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. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.

	o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o 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. o 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 ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych lub równoważne oraz posiadać autoryzacje producenta urządzeń. • Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie: o realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; o firma serwisująca posiada autoryzacje producenta oferowanego serwera;
Ilość	1 szt.

2. Serwer fizyczny niezbędny do zainstalowania produktu lud wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA typ 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	Sprzęt serwerowy wraz z niezbędnym oprogramowaniem
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji maksymalnie 8 dysków 2.5” • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy

	użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora • Możliwość obsługi procesorów 144 rdzeniowych • Płyta główna musi być zaprojektowana przez producenta serwera. • Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczone do instalacji pamięci • Płyta główna powinna obsługiwać do 1.5TB pamięci RAM.
Procesor	Zainstalowany min. jeden procesor min. 16-rdzeniowy, min. 3.6GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 206 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	• Minimum 128GB pamięci RAM DDR5 RDIMM 6400MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający: o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących o Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	• Zainstalowane: o Min. 4x dysk SSD SATA o pojemności min. 960GB, Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1
Gniazda PCI	• Minimum dwa sloty PCIe Gen5
Interfejsy sieciowe/FC/SAS	• Min. 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Min. Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28
Wbudowane porty	• Min. 4 porty USB w tym min: o 1 port USB 2.0 Type-C o 2 porty USB 3.1 o 1 port USB 3.0 wewnątrz obudowy • Min. 1 Port VGA z tyłu obudowy
Video	• Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200
Zasilacze	• Redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium.
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych

System operacyjny / dodatkowe oprogramowanie	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i minimum czterech 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, II. Umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów III. Umożliwiają kompresie „w locie" dla wybranych plików i/lub folderów, IV. 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 II. 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, III. Zdalna dystrybucja oprogramowania na stacje robocze, IV. 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) VI. 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
Wentylatory	• Redundantne

Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • 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).
Karta zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika o możliwość podmontowania zdalnych wirtualnych napędów o wirtualną konsolę z dostępem do myszy, klawiatury o wsparcie dla IPv6 o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer

	o integracja z Active Directory o możliwość obsługi przez ośmiu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej o możliwość podłączenia lokalnego poprzez złącze RS-232. o możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. o Monitorowanie zużycia dysków SSD o możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, o Automatyczne zgłaszanie alertów do centrum serwisowego producenta o Automatyczne update firmware dla wszystkich komponentów serwera o Możliwość przywrócenia poprzednich wersji firmware o Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON o Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych o Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. o Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera o Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. Możliwość rozszerzenia funkcjonalności karty o: 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. o kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania o Automatyczne odświeżanie certyfikatów SSL o możliwość wykorzystania tokenu do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej

	o możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień o możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera o możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer o możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe o monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

	o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o 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, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. o Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

	• Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.

	▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware: o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty: o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu

	oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo: o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspieranie urządzenia: o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent: o Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności: o Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne: o Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne. • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami lub równoważne. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać

	się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.
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.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany 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 oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • 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. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania

	problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o 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. o 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 ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych lub równoważne oraz posiadać autoryzacje producenta urządzeń. • Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie: o realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; o firma serwisująca posiada autoryzacje producenta oferowanego serwera;
Ilość	1 szt.

3. Serwery do kopii zapasowych

Nazwa	Minimalne wymagania dla sprzętu
Typ	Sprzęt serwerowy wraz z niezbędnym oprogramowaniem
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji maksymalnie 12 dysków 3.5” • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora • Możliwość obsługi procesorów minimum 32 rdzeniowych

	• Płyta główna musi być zaprojektowana przez producenta serwera. • Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczone do instalacji pamięci • Płyta główna powinna obsługiwać do 1.5TB pamięci RAM.
Procesor	• Zainstalowany min. jeden procesor 8-rdzeniowy, 3.6GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku 121 w teście SPECspeed®2017_fp_base w konfiguracji jednoprocesorowej, dostępnym na stronie www.spec.org dla oferowanego serwera. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	• Minimum 64GB DDR5 RDIMM 6400MT/s,
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający: o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących o Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	• Zainstalowane: o Min. 4 dyski SAS o pojemności min. 8TB, Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	• Min. Dwa sloty PCIe • Min. Dwa sloty OCP
Interfejsy sieciowe/FC/SAS	• Min. 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Min. Dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28
Wbudowane porty	• Min. 4 porty USB w tym min: o 1 port USB 2.0 Type-C o 2 porty USB 3.1 o 1 port USB 3.0 wewnątrz obudowy • Port VGA z tyłu obudowy
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
Wentylatory	• Redundantne
Zasilacze	• Redundantne, Hot-Plug min. 800W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

	• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • 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).
Karta zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika o możliwość podmontowania zdalnych wirtualnych napędów o wirtualną konsolę z dostępem do myszy, klawiatury o wsparcie dla IPv6 o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer o integracja z Active Directory o możliwość obsługi przez ośmiu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej o możliwość podłączenia lokalnego poprzez złącze RS-232. o możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. o Monitorowanie zużycia dysków SSD

	o możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, o Automatyczne zgłaszanie alertów do centrum serwisowego producenta o Automatyczne update firmware dla wszystkich komponentów serwera o Możliwość przywrócenia poprzednich wersji firmware o Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON o Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych o Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. o Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera o Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. Możliwość rozszerzenia funkcjonalności karty o: 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 . o kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania o Automatyczne odświeżanie certyfikatów SSL o możliwość wykorzystania tokenu do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej o możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień o możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera o możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer o możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe o monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

	o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o 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, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart

	sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. o Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń

	o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny

	▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware: o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty: o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo: o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.

	o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia: o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent: o Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności: o Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne: o Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami lub równoważne. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.
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.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany 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 oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • 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. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o 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. o 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 ISO 9001:2015 oraz ISO-27001 lub równoważna świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. • Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, że serwis oferowanego serwera będzie: o realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; o firma serwisująca posiada autoryzacje producenta oferowanego serwera;
Ilość	2 szt.

4. Network Attached Storage (NAS) – Siedziba Główna

Nazwa	Minimalne wymagania dla sprzętu
Typ	Network Attached Storage (NAS)
Specyfikacja sprzętowa	Procesor: Procesor w architekturze 64 bit x86 o taktowaniu nie mniejszym niż 2.8Ghz Liczba rdzeni procesora: nie mniej niż 8 Pamięć RAM: nie mniej niż 8GB DDR4 Pamięć RAM liczba slotów: min. 2 sloty Pamięć RAM możliwości rozszerzenia: nie mniej niż do 64GB Pamięć Flash: nie mniej niż 5GB Gniazdo M.2: minimum 2 Liczba zatok na dyski twarde: minimum 8 Obsługiwane dyski twarde: 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5” SSD SATA Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej 4 Porty LAN 2,5 GbE: minimum 2 Diody LED: minimum Status, LAN, HDD Porty USB 3.2 Gen 2: minimum 4 Port PCiE: minimum 2 Gen 3 x4

	Przyciski: Reset, Zasilanie Typ obudowy: RACK, maksymalnie 2U Dopuszczalna temperatura pracy minimum: od 0 do 40°C Wilgotność względna podczas pracy minimum: 5-95% R.H. Zasilanie: zasilacz redundantny maksymalnie 2 x 300 W, 100-240 V
Specyfikacja oprogramowania	Agregacja łączy: tak Obsługiwane systemy plików: • Dyski wewnętrzne: EXT4 • Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ Możliwość podłączenia karty WLAN na USB Szyfrowanie wolumenów: Tak, minimum AES 256. 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 iSCI • Multi-LUNs na Targe • 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 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, 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 SM • 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 • System plików dziennika • Całkowity rejestr systemowy (poziom pliku) • Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line • Aktualizacja oprogramowania • Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu Zabezpieczenia • Filtracja IP • Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie geolokalizacji. • Połączenie HTTPS • FTP z SSL/TLS (Explict) • 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.
Zainstalowane dyski	Minimum 8 dysków spełniające poniższe wymagania: • Pojemność minimum 6TB każdy, • Typ dysku: HDD • Interfejs dysku: SATA III • Gwarancja: minimum 36 miesięcy
Gwarancja	Minimum 36 miesięcy gwarancji producenta.

Ilość	2 szt.

5. Network Attached Storage (NAS)- pozostałe jednostki

Nazwa	Minimalne wymagania dla sprzętu
Typ	Network Attached Storage (NAS)
Specyfikacja sprzętowa	Procesor: Procesor w architekturze 64 bit x86 o taktowaniu nie mniejszym niż 2.2Ghz Liczba rdzeni procesora: nie mniej niż 4 Pamięć RAM: nie mniej niż 8GB DDR4 Pamięć RAM liczba slotów: min. 2 sloty Pamięć RAM możliwości rozszerzenia: nie mniej niż do 64GB Pamięć Flash: nie mniej niż 5GB Liczba zatok na dyski twarde: minimum 4 zatoki 3.5” Obsługiwane dyski twarde: 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5” SSD SATA Możliwość podłączenia modułu rozszerzającego: Tak, co najmniej 4 Porty LAN 2,5 GbE: minimum 2x RJ-45 Diody LED: minimum Status, LAN, HDD Porty USB 3.2 Gen 2: minimum 3 Port PCiE: minimum 2 Gen 3 x4 Przyciski: Reset, Zasilanie Typ obudowy: RACK, maksymalnie 2U Dopuszczalna temperatura pracy minimum: od 0 do 40°C Wilgotność względna podczas pracy minimum: 5-95% R.H. Zasilanie: zasilacz redundantny maksymalnie 2 x 300 W, 100-240 V
Specyfikacja oprogramowania	Agregacja łączy: tak Obsługiwane systemy plików: • Dyski wewnętrzne: EXT4 • Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ Możliwość podłączenia karty WLAN na USB Szyfrowanie wolumenów: Tak, minimum AES 256. Zarządzanie dyskami: • Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 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 iSCI • Multi-LUNs na Targe • 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 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, 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 SM • 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 • System plików dziennika • Całkowity rejestr systemowy (poziom pliku)

	• Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line • Aktualizacja oprogramowania • Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu Zabezpieczenia • Filtracja IP • Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie geolokalizacji. • Połączenie HTTPS • FTP z SSL/TLS (Explict) • 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.
Zainstalowane dyski	Minimum 4 dyski spełniające poniższe wymagania: • Pojemność minimum 8 TB każdy, • Typ dysku: HDD • Interfejs dysku: SATA III • Gwarancja: minimum 36 miesięcy
Gwarancja	Minimum 36 miesięcy gwarancji producenta.
Ilość	2 szt.

6. UTM- Unified Threat Protection -do Siedziby Głównej wraz z analiza protokołów przemysłowych OT (IT/OT) typ 1

Nazwa	Minimalne wymagania dla sprzętu
Typ	UTM Unified Threat Management- urządzenie klasy UTM ze wsparciem technicznym
Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z

	funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. Zamawiający wymaga dostawy dwóch urządzeń UTM pracujących w konfiguracji klastra wysokiej dostępności (High Availability, HA) w trybie active-passive, zapewniającym automatyczne przejęcie ruchu przez urządzenie zapasowe w przypadku awarii urządzenia podstawowego. Oferowane rozwiązanie musi umożliwiać synchronizację konfiguracji, polityk bezpieczeństwa, sesji oraz pozostałych parametrów niezbędnych do zachowania ciągłości pracy systemu bezpieczeństwa. Wykonawca zobowiązany jest do wykonania pełnej konfiguracji klastra, uruchomienia rozwiązania oraz przeprowadzenia testów poprawności działania mechanizmu przełączania awaryjnego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, dysk, zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portami Gigabit Ethernet RJ-45 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje systemu bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.

	• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

	4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

	5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe i funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów

	wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do 31.12.2026. • Ochrona systemów przemysłowych SCADA na okres do 31.12.2026.
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.
Ilość	1 kpl.

7. UTM- Unified Threat Protection do lokalizacji zdalnych wraz z analiza protokołow przemysłowych OT (IT/OT) typ 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	UTM- Unified Threat Protection do lokalizacji zdalnych wraz z analiza protokołów przemysłowych OT (IT/OT).
Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z

	funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 4 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw

	(np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 450 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje systemu bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP. • Zarządzanie pasmem (QoS, Traffic shaping). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. • Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.

	Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. Element systemu realizujący funkcję Firewall integruje się z rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

	• Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection). • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox

	realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

	System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji

	z usługą katalogową oraz zastosowaniem innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

	W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. Możliwość włączenia logowania per reguła w polityce firewall. System zapewnia możliwość logowania do serwera SYSLOG. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen do dnia 31.12.2026. • Ochrona systemów przemysłowych na okres do 31.12.2026.
Ilość	3 szt.

8. Zarządzalne urządzenia sieciowe (switch) typ 1

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe (przełączniki) -typ 1
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona aktywnie (z użyciem wentylatorów).
Porty	Minimum 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at, minimum 4 porty SFP/SFP+ 1/10GbE, Budżet mocy PoE min. 400 W Minimum 1 port typu out-of-band management Minimum 1 port konsolowy RS232 RJ45 Minimum 1 port typu USB A do transferu plików
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity min. 176 Gbps Forwarding rate min. 120 Mpps

	Pamięć flash min. 128 MB Pamięć RAM min. 512 MB
Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa minimum 8 grup LACP i minimum 8 portów fizycznych per grupa Obsługa ramek Ethernet typu Jumbo min. 9k
Funkcjonalność warstwy III	Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 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 Querier IGMP Proxy PVST/PVRST BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Private VLAN Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p (CoS) Traffic shaping/metering OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP) Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6 TFTP, FTP, Telnet, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on premise lub chmurowej
Zgodność z protokołami	802.1ab LLDP ANSI/TIA-1057- LLDP-MED 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority 802.1Q VLAN Tagging

	802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2132 DHCP options and BOOTP vendor extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Inne	Przystosowanie do pracy w temperaturze 0-50 stopni Celsjusza
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta. Bezpłatny dostęp do aktualizacji oprogramowania.
Ilość	2 szt.

9. Zarządzalne urządzenia sieciowe (switch) typ 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe (przełączniki) -typ 2
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona pasywnie.
Porty	Minimum 48 portów 10/100/1000 Mbps RJ45 minimum 4 porty SFP/SFP+ 1/10GbE, Minimum 1 port typu out-of-band management Minimum 1 port konsolowy RS232 RJ45 Minimum 1 port typu USB A do transferu plików
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity min. 176 Gbps Forwarding rate min. 120 Mpps Pamięć flash min. 128 MB Pamięć RAM min. 512 MB

Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa minimum 8 grup LACP i minimum 8 portów fizycznych per grupa Obsługa ramek Ethernet typu Jumbo min. 9k
Funkcjonalność warstwy III	Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 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 Querier IGMP Proxy PVST/PVRST BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Private VLAN Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p (CoS) Traffic shaping/metering OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP) Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6 TFTP, FTP, Telnet, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on premise lub chmurowej
Zgodność z protokołami	802.1ab LLDP ANSI/TIA-1057- LLDP-MED 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority 802.1Q VLAN Tagging 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP)

	802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2132 DHCP options and BOOTP vendor extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Inne	Przystosowanie do pracy w temperaturze 0-50 stopni Celsjusza
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta. Bezpłatny dostęp do aktualizacji oprogramowania.
Ilość	1 szt.

10. Zarządzalne urządzenia sieciowe (switch) typ 3

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe (przełączniki) -typ 3
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona pasywnie (bez użycia wentylatorów).
Porty	Minimum 24 porty 10/100/1000 Mbps RJ45, minimum 4 porty SFP/SFP+ 1/10GbE, Minimum 1 port typu out-of-band management Minimum 1 port konsolowy RS232 RJ45 Minimum 1 port typu USB A do trasferu plików
Wydajność przełącznika	Minimum 16000 adresów MAC Switch fabric capacity min. 128 Gbps Forwarding rate min. 120 Mpps Pamięć flash min. 128 MB Pamięć RAM min. 512 MB

Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa minimum 8 grup LACP i minimum 8 portów fizycznych per grupa Obsługa ramek Ethernet typu Jumbo min. 9k
Funkcjonalność warstwy III	Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 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 Querier IGMP Proxy PVST/PVRST BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Private VLAN Port Mirroring Port Security/MAC Locking DiffServ support DSCP and 802.1p (CoS) Traffic shaping/metering OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP) Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6 TFTP, FTP, Telnet, SSH v2 SNMP v1/v2/v3 Zarządzanie IPv6 Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych Zero-touch deployment Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on premise lub chmurowej
Zgodność z protokołami	802.1ab LLDP ANSI/TIA-1057- LLDP-MED 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority 802.1Q VLAN Tagging 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP)

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"

	802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3u Fast Ethernet (100BASE-TX) 802.3x Flow Control RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2132 DHCP options and BOOTP vendor extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog
Inne	Przystosowanie do pracy w temperaturze 0-50 stopni Celsjusza
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta. Bezpłatny dostęp do aktualizacji oprogramowania.
Ilość	2 szt.

11. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa typ 1

Nazwa	Minimalne wymagania dla sprzętu
Typ	Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa
Wymagania ogólne	Zamawiający wymaga dostarczenia wolnostojącej szafy instalacyjnej typu RACK 19" o wysokości minimalnej 42U przeznaczonej do montażu urządzeń teleinformatycznych i serwerowych.
Wymagania techniczne	Typ: szafa instalacyjna RACK, wolnostojąca Standard montażowy: 19 cali Wysokość użytkowa: minimum 42U Wymiary wewnętrzne (szerokość x głębokość): minimalnie 800 x 1000mm Konstrukcja: metalowa Obciążenie: minimalne 800kg. Drzwi przednie: metalowe, perforowane, Panel wentylacyjny: wymagane min. 4 wentylatory 230V w górnej obudowie.

Wymagane wyposażenie	Komplet śrub, kółka z hamulcem, nóżki, zamek drzwi
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.

12. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa typ 2

Nazwa	Minimalne wymagania dla sprzętu
Typ	Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa
Wymagania ogólne	Zamawiający wymaga dostarczenia wolnostojącej szafy instalacyjnej typu RACK 19" o wysokości minimalnej 27U przeznaczonej do montażu urządzeń teleinformatycznych i serwerowych.
Wymagania techniczne	Typ: szafa instalacyjna RACK, wolnostojąca Standard montażowy: 19 cali Wysokość użytkowa: minimum 27U Wymiary wewnętrzne (szerokość x głębokość): minimalnie 800 x 1000mm Konstrukcja: metalowa Obciążenie: minimalne 800kg. Drzwi przednie: perforowane, Panel wentylacyjny: wymagane min. 4 wentylatory 230V w górnej obudowie.
Wymagane wyposażenie	Kółka z hamulcem, nóżki, panel wentylacyjny (4 wentylatory), śruby montujące, zamek przedni, zamek tylny, zestaw elementów montażowych
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.

13. Oprogramowanie antywirusowe

Nazwa	Minimalne wymagania dla sprzętu

Typ	Oprogramowanie antywirusowe
Wymagania ogólne	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 40 stanowiskach. Dostarczone licencje muszą być ważne do 31.12.2026.
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	I. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). I. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim. I. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu: • Wirus. • Trojan. • Robak.

	• Adware. • Spyware. • Dialer. • Phishing. • Backdoor. v. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji v. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się. i. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet. i. 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. i. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. x. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. x. 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. i. 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). i. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology. i. 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. v. 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). v. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS. vi. 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. i. 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. i. 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. X. 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: o Listę zainstalowanych aplikacji. o Listę usług systemowych. o Informacje o systemie operacyjnym i sprzęcie. o Listę aktywnych procesów i połączeń sieciowych. o Harmonogram systemu operacyjnego. o Szczegóły pliku hosts. o Informacje o sterownikach. X. 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. XI. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego. XII. 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. I. 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. V. 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: o tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, o tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, o tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący, o tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu V. 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. VI. 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: o Treść komunikatu. o 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: o tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, o 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: o pamięci masowe, o optyczne pamięci masowe, B. Parametry urządzenia: o numer seryjny, o producent, o model. C. Typ dostępu: o brak możliwości zapisu, o pełen dostęp, o 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: o Listę zainstalowanych aplikacji, o Listę usług systemowych, o Informacje o systemie operacyjnym i sprzęcie, o Listę aktywnych procesów i połączeń sieciowych, o harmonogram systemu operacyjnego, o Szczegóły pliku hosts, o 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: o Pamięci masowe. o Optyczne pamięci masowe. o Pamięci masowe Firewire. o Urządzenia do tworzenia obrazów. o Drukarki USB. o Urządzenia Bluetooth. o Czytniki kart inteligentnych. o Modemy. o Porty LPT/COM. o Urządzenia przenośne. B. parametry urządzenia: o Numer seryjny, o Producent, o Model. C. typ dostępu: o Brak możliwości zapisu, o Pełen dostęp, o Ostrzeżenie użytkownika, o 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: o tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące, o tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, o tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący, o 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.

Mobile 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: o Android, o iOS, o iPadOS. B. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami: o Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników), o Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), o VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), o Apple Business Manager (ABM), o 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: o konfigurację kont e-mail, o konfigurację połączeń VPN, o Konfigurację połączeń Wi-Fi, o Konfigurację listy certyfikatów, o możliwość uruchomienia trybu jednej aplikacji. B. Dla systemu Android: o blokadę wykonywania połączeń, o blokadę konfiguracji sieci Wi-Fi, o blokadę konfiguracji tuneli VPN, o zarządzenie aktualizacjami sytemu operacyjnego, o blokadę zmiany tapety urządzenia.
Mobile Threat Defense (MTD) dla systemu 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: 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	1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.

Response / eXtended Detection and Response	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: o Pobranie plików wykonywalnych. o Zestawienie połączeń TCP/IP. o Zapytania http. o 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: o Blokowanie pliku wykonywalnego. o Blokowanie pliku wykonywalnego i poddanie go kwarantannie. o Blokowanie podejrzanej biblioteki DLL. o Zakończenie procesu. o Skanowanie komputera w poszukiwaniu zagrożeń. o Wyłączenie komputera. o Izolacja sieciowa hosta dla systemów Windows oraz Linux. o 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: o Proces. o Proces nadrzędny (proces rodzica). o Nazwę procesu.

	o Ścieżkę procesu. o Wiersz polecenia. o Wydawcę. o Typ podpisu cyfrowego. o SHA-1. o SHA-2. o 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. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia. B. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej: o SHA-1. o SHA-256. C. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML. 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.
Ilość	1 szt.

14. Oprogramowanie do monitorowania infrastruktury informatycznej

Nazwa	Minimalne wymagania dla sprzętu
Typ	Oprogramowanie do monitorowania infrastruktury informatycznej

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: 1. Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). 2. Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci. 3. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.

	4. 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. 5. 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. 6. Monitorowanie serwerów WWW i adresów URL. 7. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. 8. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP). 9. Obsługa komunikatów syslog i pułapek SNMP. 10. Monitoring routerów i przełączników wg: • zmian stanu interfejsów sieciowych, • ruchu sieciowego, • podłączonych stacji roboczych, • ruchu generowanego przez podłączone stacje robocze. 11. 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: 1. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart 2. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 4. Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP 5. Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 6. Możliwość odczytania numeru seryjnego (klucze licencyjne).

	7. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 8. 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: 1. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. 2. 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. 3. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). 4. Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). 5. 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. 6. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. 7. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. 8. 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. 9. Wyświetlanie statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 10. Wyświetlanie statystyki aktywności grupy i jej członków widoczne dla menedżera grupy 11. Grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.

	13. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 14. Przypisywanie kategorii aplikacjom i stronom internetowym, możliwość stworzenia predefiniowanej listy kategorii z możliwością edycji. 15. 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: 1. 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. 2. Pobieranie listy użytkowników z usługi katalogowej, 3. Przypisywanie pracowników helpdesk do kategorii zgłoszeń. 4. Procesowanie zgłoszeń użytkowników z wiadomości e-mail. 5. Dołączanie załączników do zgłoszeń. 6. Zrzuty ekranowe (podgląd pulpitu). 7. Dystrybucję oprogramowania przez Agentów. 8. Dystrybucję oraz uruchamianie plików za pomocą Agentów. 9. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. 10. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń. 11. Planowanie nieobecności pracowników helpdesk. 12. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA). 13. Generowanie raportów obsługi helpdesk. 14. Zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu). 15. 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. 16. Oprogramowanie powinno posiadać komunikator. 17. 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: 1. 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.

	2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 4. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 5. Autoryzowanie urządzeń firmowych: pendrive'ów, dysków zewnętrznych - urządzenia nieautoryzowane. 6. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 7. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 8. Możliwość usuwania z listy znanych urządzeń tych nośników
Licencja	Licencja wieczysta na co najmniej 40 stacji roboczych. Wsparcie serwisowe producenta musi obowiązywać do 31.12.2026
Ilość	1 szt.

15. Usługa SOC (Security Operations Center) IT/OT/ICS/IIoT

Nazwa	Minimalne wymagania dla sprzętu
Typ	Usługa SOC (Security Operations Center) IT/OT/ICS/IIoT
Świadczenie usługi SOC (Security Operations Center)	Zamawiający wymaga, aby Wykonawca świadczył usługi SOC (Security Operations Center) oraz MDR (Managed Detection and Response) do 31.12.2026 r. Zamawiający wymaga, aby Wykonawca w ramach świadczenia usługi SOC (Security Operations Center) wykorzystywał oprogramowanie klasy SIEM, zapewniające realizację wymaganych funkcjonalności bezpieczeństwa, monitorowania, analizy zdarzeń oraz automatyzacji reakcji na incydenty. Zamawiający dopuszcza rozwiązania komercyjne oraz open source. W ramach realizacji zadań Wykonawca musi świadczyć usługę administracji systemem SIEM zainstalowanym na serwerze dostarczanym w ramach niniejszego postępowania obejmującą: a. Informowanie Zamawiającego o awariach Systemu SIEM, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie, b. Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa. c. Optymalizowanie konfiguracji Systemu SIEM w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji.

	d. Konfigurację Systemu SIEM w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego w Analizie Przedwdrożeniowej e. Weryfikację czy System SIEM prawidłowo analizuje logi f. Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń. W ramach usługi SoC Wykonawca będzie wysyłał Zamawiającemu informacje odnośnie pojawiających się podatności dla systemów wskazanych w ramach podłączonych źródeł logów. W ramach realizacji zadań Wykonawca przygotuje i wdroży możliwe scenariusze wystąpienia incydentów bezpieczeństwa w systemie SIEM, które zostaną zaakceptowane przez Zamawiającego. Przykładowe scenariusze, które obligatoryjnie powinny być zaimplementowane: • Bruteforce attack (atak siłowy) • Atak złośliwego oprogramowania (malware) • Atak typu DDoS • Wykrywanie usług sieciowych (Network Service Discovery) • Zdalne wykrywanie systemów (Remote System Discovery) • Pozyskiwanie informacji o systemie (System Information Discovery) • Interpreter poleceń i skryptów (Command and Scripting Interpreter) W ramach realizacji zadań Wykonawca przygotuje i wdroży scenariusze reakcji rozumiane jako zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji powinien składać się z podzadań realizujących funkcje: • **Wzbogacenia** wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez udostępnione narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji, • **Analizy** zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia, • **Wydanie rekomendacji działań** rozumianej jako zestawienie rekomendacji umożliwiających ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,

- **Informowania i raportowania** obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie SIEM w ramach Pierwszej Linii Wsparcia oraz Drugiej Linii wsparcia w trybie 24/7, 7 dni w tygodniu.

Pierwsza linia (L1) wsparcia będzie odpowiedzialna za:

a. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie z warunkami SLA:

Priorytet zdarzenia	Czas od wykrycia przez L1 do
	Podjęcia
Poważny	30 min
Wysoki	60 min
Średni	2 h
Niski	4 h

b. Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.

c. Analizę i rekomendację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.

d. Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.

e. Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji.

f. Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.

g. Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).

h. Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.

i. Przygotowywanie miesięcznych raportów wykrytych zdarzeń bezpieczeństwa.

Druga linia (L2) wsparcia będzie odpowiedzialna za:

a. Dostępność usługi dla Zamawiającego zgodnie z warunkami SLA:

Priorytet incydentu	Czas od eskalacji pierwszej linii wsparcia do L2
	Podjęcia
Poważny	30 min

Wysoki	60 min
Średni	2 h
Niski	4 h

b. Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
c. Przygotowywanie i realizację Scenariuszy użycia systemu SIEM zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
d. Przygotowanie Scenariuszy Reakcji.
e. Przygotowanie Miesięcznych raportów z realizacji prac.

W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.
Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez pierwsza linię wsparcia a czasem nadania priorytetu. Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski zgodnie z poniższym zestawieniem:
Poważny:

1. Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO;
2. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicator of Compromise (pol. Wskaźnika skompromitowania);
3. Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min);
4. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych;
5. Informacja o potencjalnym cyberzagrożeniu od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers;
6. Potwierdzona informacja o potencjalnym cyberzagrożeniu od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową;

	7. Informacja o potencjalnym cyberzagrożeniu od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 8. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 9. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; 10. Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej; 11. Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego KSC lub RODO; Wysoki: 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicators of Compromise (pol. Wskaźnika skompromitowania) na systemie chronionym; 2. Ujawnienie zestawionej sesji zwrotnej z C&C(Command & Control), trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min); 3. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej; 4. Informacja o potencjalnym cyberzagrożeniu od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; 5. Potwierdzona Informacja o potencjalnym cyberzagrożeniu od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; 6. Informacja o potencjalnym cyberzagrożeniu od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 7. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 8. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; 9. Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); 10. Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;

	Średni: 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicators of Compromise (pol. Wskaźnika skompromitowania) na systemie chronionym; 2. Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; 3. Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; 4. Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa; 5. Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie; Niski: 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa. Zamawiający wymaga każdorazowo po wystąpieniu Incydentu o priorytecie Poważnym i Wysokim Raportu Poincydentalnego nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje: • Unikalny identyfikator zdarzenia • Kiedy incydent wystąpił? • Kiedy incydent został zauważony / wykryty? • Jaki proces był sprawcą incydentu? • Co się wydarzyło? • Gdzie wydarzenie miało miejsce? • Dlaczego zdarzenie mogło wystąpić? • Jakie czynności powinny zostać przeprowadzone przez Zamawiającego w celu powstrzymania incydentu? Zamawiający wymaga, aby każdy miesiąc świadczenia Usług podsumowany został Raportem Miesięcznym wg według wzoru przedstawionego przez Wykonawcę. Wykonawca zobowiązany jest przedstawić Raport w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa. Opis incydentu powinien składać się z sekcji: • Monitorowanie cyberbezpieczeństwa : o Data świadczenia usług o Zestawienie obsłużonych incydentów

	o Identyfikator incydentu o Nazwa o Klasyfikacja priorytetu Incydentu o Dokładna data i godzina ujawienia incydentu o Statusy końcowe • Ogólne rekomendacje i zalecenia dla Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości W ramach usługi SoC Zamawiający wymaga, aby Wykonawca minimum raz w miesiącu przeprowadził spotkanie (Zamawiający dopuszcza formę zdalnego spotkania), na którym będą przedstawione oraz omówione najczęściej występujące zdarzenia wraz z propozycjami dostosowania rozwiązania SIEM celem ograniczenia występowania incydentów False Positive, czyli gdy wykryto atak lub zagrożenie, podczas gdy nie miały one miejsca.
Świadczenie usługi MDR (Managed Detection and Response)	W ramach usługi Zamawiający oczekuje, że Wykonawca obejmie szczególnym nadzorem i opieką system klasy XDR szczegółowo opisany w punkcie 13. Oprogramowanie antywirusowe Obszaru technicznego IT. Licencje i koszty systemu pozostają po stronie Zamawiającego. W ramach usługi Wykonawca będzie przez minimum 1 godzinę dziennie monitorował i reagował na zdarzenia (detekcje) wyświetlane na podstawie logów udostępnionych przez Zamawiającego ze wskazanych źródeł oraz analizował zdarzenia bezpośrednio w konsoli oprogramowania EDR. Tworzenie własnych reguł detekcji dostosowanych do specyfiki środowiska Zamawiającego. Monitorowane są w pierwszej kolejności zdarzenia (detekcje) krytyczne (czerwone) oraz ostrzegawcze (pomarańczowe). Zamawiający zapewni dostęp do połączenia bezpośredniego do konsol oprogramowania XDR w celu zapewnienia monitorowania. Wykonawca będzie na bieżąco przekazywał rekomendacje odnośnie do dopracowania procesów bezpieczeństwa i działania infrastruktury IT Zamawiającego.
Wymagania dotyczące system SIEM (Security Information and Event Management)	Platforma przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności, spełniająca wymagania minimalne: 1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi. 2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.

	3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach. 4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI; 5. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. 6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie. 7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych. 9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware. 10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. 11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji. 12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX. 13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności

	od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora. 14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej. 15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B. 16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie. 17. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów. 18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe. 19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej. 20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych. 21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach. 22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki

	wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne. 23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa. 24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie" na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów. 25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej. 26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług. 27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły. 28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego. 29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: a) nowe zasoby wykryte w sieci, b) typy wykrytych zasobów (np.: serwer lub stacja robocza),

	c) zastosowane na nich zabezpieczenia, d) usługi z którymi się komunikują, e) nowe usługi wykryte na zasobie f) komunikację do usług wykrytych na zasobie. 30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację. 31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora. 32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy. 33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników: a) fqdn, b) e-mail, c) nazwa pliku, d) ścieżka do pliku, e) hash, f) adres IP, g) klucz rejestru, h) cmd. 34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/). 35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu). 36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs", „Malicious domain" czy „Tor Exit Nodes"). 37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

	38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. 39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu). 40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT. 41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu. 42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie. 43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności: a) id techniki, b) taktykę, c) platformy których dotyczy, d) potencjalne źródła, e) opis zagrożenia, f) mityzację, g) sposób detekcji, h) referencje. 44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. 45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych

	mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy). 46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: a) rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, b) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, c) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, d) rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów. 47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA). 48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji. 49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet). 50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. 51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację. 52. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: a) sparsowane pola oraz ich wartości, b) listy referencyjne, c) atrybuty użytkowników z Active Directory, d) atrybuty komputerów z Active Directory,

	e) bazę wskaźników kompromitacji (IOC), f) informacje z elektronicznej dokumentacji, g) anomalie w zachowaniu użytkowników (UBA), h) anomalie w zachowaniu zasobów (EBA), i) podatności na zasobach, j) wyniki analizy konfiguracji, k) techniki MITRE ATT&CK®, 53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić: a) wykrycie dowolnej treści w logach, b) wykrycie zmiany jednego z kilku pól, c) wykrycie zaniku wiadomości, d) wykrycie nowej wartości pola w zadanym okresie czasu, e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu, m) wykrycie skanowania portów. 54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: a) wykrycie wystąpienia wartości pola na wybranej liście, b) wykrycie niewystępowania wartości pola na wybranej liście, c) wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony), d) wykrycie niewystąpienia pary wartości na wybranej liście e) np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył). 55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,

	c) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej. 56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej. 57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji; b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji; 58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, c) wykrycie nieautoryzowanej usługi na serwerze, d) wykrycie nieautoryzowanego połączenia do usługi na serwerze, e) wykrycie nieautoryzowanego połączenia z serwera usług, f) wykrycie nieautoryzowanego połączenia do sieci Internet. 59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

	60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach. 61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, c) wykrycie zdarzeń o wysokim „severity" na zasobach posiadającego krytyczne podatności, d) wykrycie zdarzeń o wysokim „severity" do zasobów posiadających krytyczne podatności. 62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na: a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić: a) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, b) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, c) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie. 64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.: a) wykrycie anomalii na koncie uprzywilejowanym użytkownika, b) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,

	c) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, d) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, e) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny 65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać: a) sparsowane pola oraz ich wartości, b) atrybuty użytkowników z Active Directory, c) atrybuty komputerów z Active Directory, d) informacje z elektronicznej dokumentacji. 66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: a) adresie IP, b) koncie domenowym użytkownika, c) strefie bezpieczeństwa, d) zakresie adresów IP. 67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop" umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej. 68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze. 69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.: a) wszystkie skorelowane zdarzenia, b) korespondencja pocztowa,

	c) załączniki z próbkami lub dowodami, d) wskaźniki kompromitacji (IoC), e) informacje pozyskane z innych systemów. 70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora. 71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa. 72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: a) identyfikację celu i źródła zagrożenia, b) nazwę oraz adres IP źródła zagrożenia, c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, d) lokalizację z które pochodzi zagrożenie np.: Internet, e) strefę bezpieczeństwa z której pochodzi zagrożenie, f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), h) nazwę oraz adres IP celu zagrożenia, i) zabezpieczenia lokalne chroniące cel zagrożenia, j) strefę bezpieczeństwa w której znajduje się cel zagrożenia. 73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall). 74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami.

	Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem. 75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: a) nazwy zasobu, b) rodzaju zasobu, c) ważności zasobu dla organizacji, d) rodzaj przetwarzanych informacji, e) usług, które ten zasób świadczy, f) lokalizację użytkowników, którzy z niego korzystają, g) usługi z których zasób korzysta. 76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych. 77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: a) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, b) segregacja – segregacja i kwalifikacja zdarzeń, c) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, d) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, e) zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. 78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi. 79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę

	statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych. 80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów. 81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów. 82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów. 83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API. 84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: a) podgląd aktywności zagrożonego zasobu na linii czasu, b) w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, c) w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, d) podgląd reguły korelacyjnej, która wygenerowała zdarzenie, e) w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis, f) listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, g) gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o: • listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, • listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym, h) gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:

	• listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, • listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym. 85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a) warunki powiadomień: • zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, • zdarzeń o przekroczonych czasach SLA o definiowalny okres, • zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, • zdarzeń, których priorytet osiągnął określoną wartość, • zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, • zdarzeń na których doszło do naruszenia bezpieczeństwa, • zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, • zdarzeń realizujących zdefiniowaną usługę, • zdarzeń przetwarzających sklasyfikowane informację, • zdarzeń przetwarzanych na krytycznych zasobach, b) odbiorców powiadomień, w tym: • operatora, któremu zostało przydzielone zdarzenie, • właściciela zasobu na którym wystąpiło zdarzenie, • zespół obsługi, który odpowiada za obsługę zdarzeń, • właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie, • podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną. c) kanały powiadomień, m.in. e-mail, sms, komunikator, d) zastosowanie mechanizmów grupowania: • grupowanie wielu powiadomień w jednej wiadomości, • ograniczenie liczby wierszy powiadomienia do określonej wartości. 86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a) utworzenia nowego zdarzenia z określonym priorytetem, b) utworzenia nowego zdarzenia na zasobie krytycznym, c) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, d) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, e) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,

	f) modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, g) zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, h) przejęcia przydzielonego operatorowi zdarzania przez innego operatora. 87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: a) wybór raportu, który ma zostać wysłany, b) zdefiniowanie jego tytułu, c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d) możliwość ograniczenia cyklu do dni powszednich, e) określenie daty przesłania pierwszego raportu, f) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do: • zdefiniowanej daty końcowej, • określnej liczby raportów, g) określenie odbiorców raportu. 88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook). 89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry: a) strefę bezpieczeństwa w której została wykryta podatność, b) prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, c) rodzaj zasobu którego dotyczy ta podatność, d) ważność tego zasobu dla organizacji, e) przetwarzane na tym zasobie informacje, np.: dane osobowe, f) usługi realizowane przez ten zasób, np.: DNS, g) wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact" = High, h) poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, i) szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet. 90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz

	interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji. 91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: a) wyliczonym priorytecie podatności, b) aktualnym statusie obsługi, c) ważności zasobu na którym została wykryta, d) adresie IP tego systemu, e) parametrów SLA związanych z tym statusem, f) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, g) parametrach CVSS, np.: lista podatności których „Access Complexity (AC)" = „low" oraz „Access Vector (AV) = „Network". 92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach: a) przekroczenia czasu reakcji o określony czas np.: o godzinę, b) możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, c) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, d) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, e) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, f) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, g) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, h) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, i) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, j) przekroczenia czasu reakcji dla podatności na zasobie krytycznym, k) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę, 93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a) warunki powiadomień:

	• podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, • podatności o przekroczonych czasach SLA o definiowalny okres, • podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, • podatności, których priorytet osiągnął określoną wartość, • zdarzeń realizujących zdefiniowaną usługę, • zdarzeń przetwarzających sklasyfikowane informację, • zdarzeń przetwarzanych na krytycznych zasobach, b) odbiorców powiadomień, w tym: • operatora, któremu została przydzielona podatność, • właściciela zasobu na którym wystąpiła podatność, • zespół obsługi, który odpowiada za obsługę podatności, • właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność, • podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną. c) kanały powiadomień, m.in. e-mail, sms, komunikator, d) zastosowanie mechanizmów grupowania: • grupowanie wielu powiadomień w jednej wiadomości, • ograniczenie liczby wierszy powiadomienia do określonej wartości. 94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a) przydzielenia nowej podatności do obsługi z określonym priorytetem, b) przydzielenia nowej podatności do obsługi na zasobie krytycznym, c) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, d) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, e) modyfikacji przydzielonej operatorowi podatności przez innego operatora, f) zamknięcia przydzielonej operatorowi podatności przez innego operatora, g) przejęcia przydzielonej operatorowi podatności przez innego operatora. 95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na: a) wybór raportu który ma zostać wysłany, b) zdefiniowanie jego tytułu,

	c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d) możliwość ograniczenia cyklu do dni powszednich, e) określenie daty przesłania pierwszego raportu, f) określenie okresu przez jaki będą one przesyłane, poprzez: g) określenie odbiorców raportu. 96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard'u", tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika. 97. System musi pozwalać na tworzenie dedykowanych dashboard'ów obejmujących: a) zestaw wykresów dla bieżącego użytkownika, b) zestaw wykresów dla wybranego użytkownika, c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center). 98. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy: a) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia: b) wykres przedstawiający skale zagrożeń, który uwzględnia: c) wykres przedstawiający źródła zagrożeń, który uwzględnia: d) wykres przedstawiający poziom zagrożeń, który uwzględnia: e) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia: f) wykres przedstawiający zagrożone usługi, który uwzględnia: g) wykres przedstawiający zagrożone dane, który uwzględnia: h) wykres przedstawiający skale podatności, który uwzględnia: i) wykres przedstawiający czas obsługi podatności, który uwzględnia: j) wykres przedstawiający wagę podatności, który uwzględnia: 99. Nawigacja w ramach „Dashboard'u" musi wspierać opcję typu „Drill down" w następującym zakresie: a) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, b) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, c) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,

	d) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, e) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, f) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres. 100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. 101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych: a) kolektor parsujący; b) kolektor logów; c) kolektor korelacyjny; d) kolektor zdarzeń; e) kolektor sztucznej inteligencji; f) kolektor reakcyjny; g) kolektor kontrolujący. 102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń. 103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

	104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. 105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy 106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody. 107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji. 108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych. 109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe. 110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania. 111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów. 112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń

	licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej. 113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów. 114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.) 115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych. 116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych. 117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta. 118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania. 119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji. 120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB). 121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania. 122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów 123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

	124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI). 125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości: a) zdolność do definiowania wzorców które powtarzają się jako zmienne; b) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych; c) zdolność do testowania poszczególnych funkcji; d) zdolność do przekształcania danych w trakcie ich parsowania 126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości: a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej; b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; d) zdolność do monitorowania integralności plików; e) zdolność do monitorowania rejestru systemowego; f) zdolność do monitorowania urządzeń zewnętrznych (removable devices); g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS; h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS; j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu. 127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar. 128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

	129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń. 130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data). 131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi. 132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal. 133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł. 134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji. 135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów. 136. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM. 137. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego. 138. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego,

	związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć. 139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem. 140. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie. 141. Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać minimum 50 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności. 142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów. 143. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise", w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet. 144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x)
Wymagania dotyczące licencji i wsparcia	Dostarczone rozwiązanie musi być w formie licencji wieczystej oraz być objęte wsparciem producenta lub producentów minimum 31.12.2026 r. Wykonawca w ramach dostawy musi zapewnić bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 1 osoby i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez Certyfikowanego Inżyniera systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.
Wdrożenie narzędzia SIEM	Wdrożenie rozwiązania SIEM obejmuje instalację na minimum 2 maszynach wirtualnych przygotowanych przez Zamawiającego. W ramach wdrożenia system musi zostać podłączony do minimum 50 źródeł logów pochodzących z minimum: serwerów fizycznych, serwerów wirtualnych, urządzeń sieciowych, rozwiązań endpoint protection, rozwiązań DLP oraz urządzeń klasy UTM dostarczanych w niniejszym postepowaniu. Wykonawca musi przygotować harmonogram wdrożenia który obejmuje 6 etapów.

	1. Analiza przedwdrożeniowa: określenie istotnych informacji które system powinien wykrywać z podłączonych źródeł logów w ramach monitoringu, przygotowanie reguł bezpieczeństwa i implementacja na etapie konfiguracji systemu. 2. Instalacja systemu: instalacja oprogramowania według wcześniej przedstawionej architektury działania oraz wcześniej przygotowanego schematu komunikacji sieciowej w sieci lokalnej Zamawiającego 3. Konfiguracja systemu: implementacja wcześniej opracowanych reguł bezpieczeństwa wraz z weryfikacją ich działania 4. Dostrojenie systemu: dostrojenie oprogramowania tak aby nie powodowało nadmiernej ilości fałszywych alarmów 5. Szkolenia: przeprowadzenie szkolenia zawierającego elementy: codziennej obsługi zdarzeń oraz ich analizy, sposoby dodawania nowych źródeł loków, aktualizacja systemu do nowszej wersji 6. Dokumentacja powdrożeniowa: dostarczenie zamawiającemu dokumentacji powdrożeniowej, wskazującej wszystkie istotne elementy z punktu widzenia wdrożenia, wraz ze wszystkimi danymi dostępowymi do kont technicznych stworzonych na etapie wdrożenia
Wymagania wobec Wykonawcy świadczącego usługę SOC	Zamawiający wymaga, aby wykonawca posiadał waży i aktualny akredytowany (wydany przez podmiot posiadajacy akredytację PCA – Polskie Centrum Akredytacji lub instytucji równoważnej) certyfikat ISO 27001 lub równoważny oraz ISO 22301 lub równoważny dla usługi Security Operations Center . Certyfikaty należy załączyć do oferty. Wykonawca musi posiadać status co najmniej "Listed" w Trusted Introducer (TI), tj. być ujęty w katalogu zespołów reagowania na incydenty bezpieczeństwa IT prowadzonym przez TF-CSIRT/Trusted Introducer lub równoważne. Wydruk ze strony http://trusted-introducer.org/trusted-introducer/ należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim. Zamawiający wymaga, aby Wykonawca dysponował personelem z potwierdzonymi umiejętnościami osobowymi, potwierdzonymi przez poniższe certyfikaty: • minimum 1 osoba posiadająca certyfikat CompTIA Security + (The Computing Technology Industry Association Security +) lub równoważny; • minimum 1 osoba posiadająca certyfikat CompTIA CySA + (The Computing Technology Industry Association Analyst +) lub równoważny; • minimum 1 osoby posiadające certyfikat CEH (Certified Ethical Hacker) lub równoważny; • minimum 1 osoby posiadające certyfikat CIH (Certified Incident Handler) lub równoważny;

	• minimum 1 osoba posiadające certyfikat Aud Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001
Ilość	1 szt.

16. Oprogramowanie przeciwdziałające wyciekowi danych (DLP- Data Leak Prevetion)

Nazwa	**Minimalne wymagania dla sprzętu**
Typ	Oprogramowanie przeciwdziałające wyciekowi danych (DLP- Data Leak Prevetion)
Wymagania ogólne	Zamawiający wymaga dostarczenia licencji o minimalnych wymaganiach: 1. System musi być wspierany przez: A. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi B. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi C. MacOS 12 lub nowszy. 2. Serwer administracyjny musi obsługiwać instalację na systemach. 3. Serwer administracyjny musi obsługiwać bazy danych 4. Pomoc i dokumentacja programu muszą być dostępne w języku angielskim. 5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. 6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych. 8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. 9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. 10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. 11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit. 12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania. 13. Administrator musi mieć możliwość, aby tworzyć, usuwać i konta administratorów w konsoli programu. 14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). 15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.

	16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. 17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa. 18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach. 19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików. 20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. 21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email. 22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu. 23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta. 24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików. 25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. 26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich, gdzie zawartość pliku jest niemożliwa do odczytania. 27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. 28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN. 29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych 31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.

	32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. 33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. 34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365. 35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. 36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach. 37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej. 38. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia. 39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego. 40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik. 41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem. 42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej. 43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń. 44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana. 45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP.

	46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf.
Licencja	W ramach dostawy, Zamawiający wymaga dostarczenia licencji bezterminowych oprogramowania klasy DLP dla minimum 40 użytkowników wraz ze wsparciem obowiązującym do: 31.12.2026
Ilość	1 szt.

17. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa

Nazwa	Minimalne wymagania dla sprzętu
Typ	Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa
Wymagania ogólne	Moc pozorna: min. 3000VA Moc rzeczywista: min. 3000W Technologia: on-line(VFI), podwójna konwersja Sprawność: min. 90% Typ obudowy: Rack/tower
Wejście	Napięcie wejściowe: 110 ÷ 300 V AC ± 2% Częstotliwość napięcia wejściowego: 50/60 Hz Zakres częstotliwości: 40-70 Hz Współczynnik mocy: 0,99 (przy pełnym obciążeniu) Gniazdo zasilania wejściowe: IEC 320 C20
Wyjście	Zakres napięcia wyjściowego: 200 V AC / 208 V AC / 220 V AC / 230 V AC / 240 V AC ± 2 % Kształt napięcia wyjściowego: sinusoidalny Czas przełączania siec-UPS: 0ms Gniazda wyjściowe minimum: 8x IEC 320 C13, 1x IEC 320 C19 Przeciążalność: 100 ÷ 105 - ostrzeżenie (praca normalna); 105 ÷ 125 - 5 min; 125 ÷ 150 - 30 s; > 150÷ - 500 ms
Sprawność	Minimum 93%
Baterie	Typ baterii: min. 12V 9AH, Ilość baterii: minimum 6 sztuk. Czas pracy na bateriach: Przy ociążeniu 80%- min. 5 min
Interfejsy komunikacyjne	Wyświetlacz: ekran LCD oraz diody LED Złącza minimum: USB, RS232
Certyfikaty	ISO 9001:2015 dla producenta sprzętu lub równoważne obejmujący proces projektowania, produkcji i Serwisowania.
Gwarancja	Minimum 24 miesiące. Autoryzowany serwis producenta musi być zlokalizowany w Polsce. Serwis musi być realizowany w systemie door to door. Naprawa maksymalnie 5 dni roboczych.
Ilość	2 szt.

18. Wdrożenie usługi Active Directory wraz z wpięciem użytkowników do domeny

Nazwa	Minimalne wymagania dla usługi
Typ	Wdrożenie usługi Active Directory wraz z wpięciem użytkowników do domeny
Wymagania ogólne	Zamawiający w ramach realizacji przedmiotu zamówienia wymaga wdrożenia usługi katalogowej o zakresie minimum: • uruchomienie nowej instancji systemu operacyjnego Windows Serwer będącego w posiadaniu Zamawiającego, • wdrożenie, instalacja roli usługi katalogowej, • konfiguracja struktury organizacyjnej, • stworzenie podstawowych polityk GPO zgodnie z wymaganiami Zamawiającego, • utworzenie przykładowego użytkownika, • przygotowanie i dołączenie stacji roboczej/serwera do kontrolera domeny, • podstawowe szkolenie administratorów w zakresie dodawania użytkowników i dodawania stacji roboczych, zarządzanie użytkownikami i stacjami, Wykonawca wykona testowe dodanie do 5 urządzeń PC do pracy w domenie. przygotowanie dokumentacji powdrożeniowej.
Ilość	1 szt.

19. Fizyczny montaż serwerów wraz z aktualizacją oprogramowania, fizyczny montaż i konfiguracja urządzeń UPS

Nazwa	Minimalne wymagania dla usługi
Typ	Fizyczny montaż serwerów wraz z aktualizacją oprogramowania, fizyczny montaż i konfiguracja urządzeń UPS
Wymagania ogólne	Zamawiajacy wymagana fizycznego montażu serwerów w szafach RACK 19” wraz z ich Instalacją, podłączeniem do infrastruktury zasilającej i sieciowej oraz przeprowadzeniem aktualizacji oprogrmowania wewnętrzego wszystkich komponentów serwerowych do najnowszych stabilnych wersji udostępnionych przez producenta. Zamawiający wymaga fizycznego montażu zasilaczy awaryjnych UPS, podłączenia do

	infrastruktury elektrycznej i urządzeń odbiorczych, konfigurację parametrów pracy, uruchomienia systemu monitorowania oraz weryfikację poprawności działania w środowisku produkcyjnym. Wykonawca jest zobowiązany do przeprowadzenia testów funkcjonalnych po zakończeniu prac, potwierdzenia prawidłowego działania wszystkich urządzeń oraz przekazania dokumentacji powykonawczej zawierającej opis wykonanych czynności i zastosowane konfiguracje.
Ilość	1 szt.

20. Wdrożenie oprogramowania antywirusowego, wdrożenie oprogramowania do monitorowania infrastruktury informatycznej, wdrożenie oprogramowania przeciwdziałającego wyciekowi danych, wdrożenie oprogramowania do tworzenia kopii zapasowych

Nazwa	Minimalne wymagania dla sprzętu
Typ	Wdrożenie oprogramowania antywirusowego, wdrożenie oprogramowania do monitorowania infrastruktury informatycznej, wdrożenie oprogramowania przeciwdziałającego wyciekowi danych, wdrożenie oprogramowania do tworzenia kopii zapasowych
Wymagania ogólne	Wdrożenie oprogramowania antywirusowego XDR: • 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, Wdrożenie oprogramowania do monitorowania infrastruktury informatycznej: • Wykonawca zainstaluje i skonfiguruje serwer zarządzający wraz z bazą danych oraz komponentami administracyjnymi. W ramach tego etapu uruchomione zostaną funkcje skanowania i monitorowania sieci, wykrywania urządzeń i usług TCP/IP, dostępu administracyjnego oraz mechanizmów kopii zapasowej konfiguracji systemu, zgodnie z możliwościami platformy.

	• Wykonawca zainstaluje agenty na wybranych urządzeniach końcowych z pomocą mechanizmu GPO. • Wykonawca wdroży wszystkie moduły oprogramowania • Integracja z usługą katalogową i modelem uprawnień, • Testy powdrożeniowe i odbiór. Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych: • Instalacja oprogramowania DLP • Instalacja konsoli zarządzającej • Przeprowadzenie logowania do konsoli zarządzającej • Konfiguracja SMTP • Podłączenie do infrastruktury posiadanej przez Zamawiającego (Active Directory) • Wygenerowanie agenta rozwiązania DLP oraz przeprowadzenie instalacji na środowiskach testowych wybranych przed wdrożeniem • Przypisanie licencji • Konfiguracja raportowania i monitorowania • Utworzenie stref bezpiecznych i niebezpiecznych • Instalacja klienta na stacjach z zainstalowanym agentem • Utworzenie reguł DLP wcześniej skonsultowanych z Zamawiającym • Wykonanie testów
Ilość	1 kpl.

21. Centralny manager haseł w wersji On-Premise

Nazwa	Minimalne wymagania dla sprzętu
Typ	Centralny manager haseł w wersji On-Premise
Wymagania ogólne	Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego licencji na oprogramowanie zarządzalnego menedżera haseł z możliwością udostępniania i współpracy w zakresie wymiany danych dostępowych. I. 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 40 użytkowników.

	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 być dostępne minimum w języku polskim i angielskim z możliwością zmiany języka z poziomu organizacji oraz indywidualnego użytkownika. 6. Oprogramowanie musi posiadać architekturę klient/serwer z umożliwieniem uruchomienia jej w opcji on-premise. 7. Oprogramowanie musi spełniać normy dostępności treści internetowych dla osób niepełnosprawnych min. w zakresie wyboru kroju czcionki, wyboru rozmiaru czcionki oraz możliwości czytania tekstu. II. Minimalne wymagania dotyczące przechowywania danych: 1. Oprogramowanie musi umożliwić tworzenie, modyfikowanie i usuwanie wpisów z danymi dostępowymi składającymi się z minimum: a) Tytułu, b) Loginu, c) Hasła, d) Adresu URL strony, e) Daty wygaśnięcia, f) Notatki. 2. Oprogramowanie musi umożliwiać tworzenie, modyfikowanie i usuwanie wpisów z danymi kart kredytowej składających się z minimum: a) Tytułu, b) Numeru karty, c) Daty wygasania, d) Numeru CVV, e) Pinu, f) Właściciela karty, g) Notatki. 3. Oprogramowanie musi umożliwiać tworzenie, modyfikowanie i usuwanie wpisów dedykowanych do przechowywania notatek składających się z minimum: a) Tytułu, b) Treści notatki, 4. Oprogramowanie musi umożliwić dodawanie wpisów z danymi dostępowymi bez konieczności podawania wszystkich pól wymienionych w punkcie 1.

	5. Oprogramowanie musi umożliwić nadawanie etykiet na wpisy, umożliwiając przy tym wizualną identyfikację przynależności do danej etykiety. 6. Oprogramowanie musi umożliwić dodawanie załączników do wpisów w formie plików z możliwością zdefiniowania dozwolonych rozszerzeń i rozmiarów w licencji. 7. 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. 8. Oprogramowanie musi umożliwić dostosowywanie grup dostępowych poprzez nazwy oraz ikony. 9. Oprogramowanie musi umożliwić tworzenie grup prywatnych, do których dostęp ma jedynie właściciel. 10. Oprogramowanie musi umożliwić tworzenie grup współdzielonych, do których dostęp ma właściciel i wszyscy uprawnieni użytkownicy wskazani przez właściciela. 11. Oprogramowanie musi mieć możliwość wyszukiwania wpisów po tytule. 12. 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. 13. Oprogramowanie musi udostępniać wskaźnik siły haseł przechowywanych na koncie użytkownika. 14. Oprogramowanie musi umożliwiać udostępnianie haseł w obrębie organizacji wykorzystując mechanizm grup współdzielonych. 15. Oprogramowanie musi umożliwiać jednorazowe udostępnianie haseł dla użytkowników spoza organizacji za pomocą tymczasowych linków z ważnością czasową. 16. Oprogramowanie musi umożliwiać import haseł z innych menedżerów haseł, minimum: a) Google Chrome, b) Mozilla Firefox, c) Apple Safari, d) Opera, e) KeePass. 17. Podczas importu należy zachować podział na grupy lub foldery zgodnie ze strukturą pliku źródłowego. W przypadku zagnieżdżonych grup lub folderów dopuszcza się spłaszczenie ich struktury.

	18. Oprogramowanie musi umożliwiać użytkownikowi eksport wpisów przechowywanych w menedżerze haseł, umożliwiać wykonanie kopii, archiwizacji lub migracji danych do innego rozwiązania. 19. Oprogramowanie musi umożliwiać eksport wpisów należących do wybranej grupy wpisów albo innego logicznego zbioru danych wskazanego przez użytkownika. 20. Eksport wpisów musi odbywać się z uwzględnieniem uprawnień użytkownika. 21. Oprogramowanie musi umożliwiać eksport co najmniej: a) w natywnym formacie oferowanego rozwiązania. b) w co najmniej jednym formacie niezależnym od oferowanego rozwiązania, który: o musi być plikiem szyfrowanym oraz zabezpieczonym hasłem o musi umożliwiać przenoszenie danych uwierzytelniających pomiędzy rozwiązaniami. o musi być publicznie udokumentowany lub powszechnie obsługiwany przez niezależne narzędzia do zarządzania hasłami. o musi umożliwiać import albo odczyt danych w innym rozwiązaniu bez konieczności modyfikacji struktury pliku oraz bez konieczności korzystania z narzędzi dostawcy oferowanego rozwiązania. 22. Oprogramowanie musi udostępniać możliwość przeglądania załączników do haseł za pomocą dedykowanego widoku na portalu. 23. Oprogramowanie musi automatycznie weryfikować i oznaczać hasła, które pojawiły się w publicznych bazach wycieków danych. Hasła, które „wyciekły” muszą być wyraźnie oznaczone umożliwiając ich identyfikację oraz natychmiastową zmianę. 24. Oprogramowanie musi udostępniać ogólny wskaźnik siły haseł dla administratorów. 25. Oprogramowanie musi umożliwiać nadawanie miękkich (nieblokujących możliwości dodawania / edycji wpisów) wymagań na hasła z grup współdzielonych oraz wyświetlać ewentualne naruszenia w panelu administratora. III. 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 administratora organizacji, managerów oraz użytkowników. 3. Oprogramowanie musi mieć możliwość wdrożenia w środowisku informatycznym Zamawiającego i dawać możliwość integracji z Active Directory.

	4. Oprogramowanie musi umożliwiać nadawanie dostępu do całych grup współdzielonych w formie opcji zarządzania, zarządzania z możliwością dalszego udostępniania 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 umożliwiać nadawanie i odbieranie przywilejów do tworzenia grup współdzielonych i/lub personalnych dla użytkowników. 8. Oprogramowanie musi umożliwiać dostęp do logów systemowych, zbierających informacje o aktywności użytkowników w zakresie minimum: a) Aktywacji konta, b) Zmiany danych dostępowych konta, c) Udanych oraz nieudanych prób logowania, d) Tworzenia/modyfikacji/usuwania grup/wpisów, e) Momentu otrzymania / utraty dostępu do grupy wpisów. f) Zdarzeń dotyczących administrowania użytkownikami, g) Udostępniania grup oraz wpisów wewnątrz oraz na zewnątrz organizacji 9. Oprogramowanie musi umożliwiać przesyłanie logów systemowych do zewnętrznego systemu zarządzania logami z wykorzystaniem protokołu Syslog 10. Logi systemowe muszą jednoznacznie identyfikować użytkownika oraz urządzenie, z którego wykonywane są zdarzenia, minimum poprzez zapisanie nazwy użytkownika, nazwy urządzenia oraz adresu IP. 11. Oprogramowanie musi umożliwiać eksport logów do formatu minimum .csv z możliwością definicji zakresu czasowego, typu logów czy użytkownika, którego dotyczą. 12. Oprogramowanie musi umożliwiać monitorowanie i zarządzanie aktywnymi sesjami użytkownika, a także pozwalać na zamknięcie wszystkich istniejących. IV. Minimalne wymagania dotyczące szyfrowania: 1. Oprogramowanie musi umożliwiać nadanie dwóch niezależnych haseł użytkownika, jedno do konta użytkownika, drugie do szyfrowania/odszyfrowania danych dotyczących haseł. 2. Oprogramowanie musi umożliwiać zmianę i reset hasła do konta. 3. Oprogramowanie musi umożliwiać zmianę hasła wykorzystywanego do szyfrowania/odszyfrowania danych dotyczących haseł.

	4. Oprogramowanie musi stosować minimum funkcję PBKDF2 na poziomie minimum 800000 iteracji. 5. Oprogramowanie musi stosować szyfrowanie symetryczne oraz asymetryczne w procesie zabezpieczania wpisów z hasłami, wykorzystując klucze min. RSA o długości minimum 2048 bitów oraz szyfrowania min. AES w trybie GCM. 6. Oprogramowanie musi umożliwić użytkownikowi nadania sobie weryfikacji dwuetapowej w postaci minimum: a) Kodu SMS, b) Kodu e-mail, c) Kodu w aplikacji zewnętrznego dostawcy (np. Google Authenticator, Microsoft Authenticator), d) Sprzętowych kluczy zabezpieczających. V. Minimalne wymagania dotyczące wtyczki do przeglądarki: 1. Oprogramowanie musi umożliwić pobranie i uruchomienie wtyczki w przeglądarkach minimum: a) Google Chrome, b) Mozilla Firefox, c) 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 otworzenie wtyczki w nowym oknie. 6. Oprogramowanie musi umożliwiać automatyczne proponowanie dodawania wpisów w przypadku wykrycia logowania na nowym portalu. 7. Oprogramowanie musi umożliwiać automatycznie proponować generowanie silnych haseł w przypadku wykrycia rejestracji na nowym portalu. 8. Oprogramowanie musi umożliwiać przeglądanie posiadanych wpisów wraz z możliwością kopiowania poszczególnych danych. 9. 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. 10. Oprogramowanie musi umożliwiać aktualizację wpisów w przypadku wykrycia zmiany hasła na portalu.

	11. Oprogramowanie musi umożliwiać funkcjonalność automatycznego wypełniania pól formularza logowania za pomocą nakładki loginem i hasłem dodanym wcześniej do banku haseł. VI. Minimalne wymagania dotyczące aplikacji mobilnej: 1. Oprogramowanie musi umożliwić pobranie i uruchomienie aplikacji minimum na systemach mobilnych w sklepach: a) Google Play na urządzenia mobilne z systemem Android, b) 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 i edycję 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. 7. Oprogramowanie musi umożliwiać obsługę kodów TOTP poprzez generowanie jednorazowych kodów, skanowanie kodów QR oraz manualne wprowadzanie kodów sekret. 8. Oprogramowanie musi powiadamiać użytkownika o nowych dostępach udostępnionych dla niego przez innych użytkowników. 9. Oprogramowanie musi umożliwiać udostępnianie grup orazpojedynczych wpisów. VII. Minimalne wymagania w zakresie: licencjonowania, wsparcia technicznego oraz aktualizacji: 1. Licencja musi obejmować prawo do użytkowania na czas nieokreślony. 2. Wsparcie techniczne musi być świadczone bezpośrednio przez producenta do dnia 31.12.2026. 3. Wsparcie techniczne musi być realizowane w języku polskim. 4. Zakładanie zgłoszeń (tzn. tickety) musi być możliwe za pośrednictwem dedykowanych kanałów komunikacji tj. adresu e-mail lub bezpośredniego numeru telefonu producenta. 5. Producent wraz z rozwiązaniem musi udostępniać materiały samouczące w j. polskim - minimum w postaci bazy wiedzy. 6. Wsparcie techniczne obejmuje dostęp do bieżących aktualizacji oprogramowania przeprowadzanych przez producenta każdorazowo po uzgodnieniu terminu z Zamawiającym.

	7. W przypadku wystąpienia awarii, producent zobowiązany jest, w ramach świadczonego wsparcia technicznego i bez dodatkowych opłat, do podjęcia działań serwisowych, mających na celu przywrócenie ciągłości działania systemu. VIII. Minimalne wymagania w zakresie wdrożenia oraz szkolenia: 1. Wykonawca dokona instalacji wymaganych komponentów systemu na wskazanym przez Zamawiającego serwerze lub maszynie wirtualnej. 2. Wykonawca dokona konfiguracji licencji oraz utworzy konto głównego administratora systemu, umożliwiając Zamawiającemu korzystanie z funkcjonalności oprogramowania. 3. Po zakończeniu instalacji Wykonawca przeprowadzi testy uruchomieniowe w celu potwierdzenia poprawnego działania systemu i jego gotowości do użytkowania, 4. Wykonawca zapewni szkolenie obejmujące zarówno obsługę użytkownika, jak i administrowanie wdrożonym systemem.
Ilość	1 szt.

22. Klucze sprzętowe U2F

Nazwa	Minimalne wymagania dla sprzętu
Typ	Klucze sprzętowe U2F
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	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, Xbox Live),
Wymagania Bezpieczeństwa	1. Klucz musi wykorzystywać mechanizmy kryptograficzne oparte o klucze 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	Urządzenie musi być zgodne ze standardami FIDO Alliance: • FIDO2 • FIDO U2F
Gwrancja	24 miesiące gwarancji producenta
Ilość	1 szt

III. OBSZAR TECHNICZNY OT

23. Separacja sieci IT/OT, wdrożenie urządzeń UTM, instalacja i wdrożenie przełączników sieciowych

Nazwa	Minimalne wymagania dla usługi
Typ	Separacja sieci IT/OT, wdrożenie urządzeń UTM, instalacja i wdrożenie przełączników sieciowych
Wymagania ogólne	Zamawiający wymaga przeprowadzenia usług: Wykonanie separacji sieci:

	• wydzielenie logiczne i/lub fizyczne sieci IT oraz OT, • opracowanie i wdrożenie odpowiedniej architektury segmentacji sieci, • zastosowanie mechanizmów VLAN, ACL, stref bezpieczeństwa oraz innych mechanizmów kontroli dostępu, stosownie do wymagań Zamawiającego, • ograniczenie komunikacji pomiędzy środowiskami IT i OT wyłącznie do niezbędnych, zdefiniowanych usług i protokołów, • wdrożenie zasad minimalizacji dostępu zgodnie z zasadą least privilege. Dostawy, instalacji i wdrożenia urządzeń UTM: • montaż urządzeń w miejscu wskazanym przez Zamawiającego, • wykonanie niezbędnych połączeń sieciowych, • konfigurację interfejsów, stref bezpieczeństwa, routingu oraz reguł bezpieczeństwa, • konfigurację funkcji zapory sieciowej (Firewall), • konfigurację mechanizmów kontroli i filtrowania ruchu pomiędzy sieciami IT i OT, • wdrożenie, w zakresie obsługiwanym przez dostarczone urządzenia, mechanizmów IPS/IDS, filtrowania aplikacji, kontroli dostępu oraz ochrony przed zagrożeniami sieciowymi, • konfigurację rejestrowania zdarzeń i logów oraz mechanizmów monitorowania stanu urządzeń, • konfigurację bezpiecznego dostępu administracyjnego, • wykonanie testów poprawności działania oraz testów skuteczności wdrożonych mechanizmów separacji. Instalacji i wdrożenia przełączników sieciowych: • montaż przełączników w szafach/rackach lub innych miejscach wskazanych przez Zamawiającego, • wykonanie i uporządkowanie połączeń kablowych, • konfigurację VLAN oraz przypisanie portów do odpowiednich segmentów sieci, • konfigurację trunków, agregacji łączy oraz mechanizmów redundancji, jeżeli są wymagane w projekcie, • konfigurację mechanizmów zabezpieczających porty dostępowe, w szczególności kontroli dostępu do sieci oraz ograniczenia nieautoryzowanych urządzeń, • konfigurację parametrów zarządzania, monitorowania i diagnostyki, • aktualizację oprogramowania systemowego urządzeń do wspieranej i zalecanej przez producenta wersji, • opisanie i oznakowanie portów oraz połączeń zgodnie z przyjętą dokumentacją.

	Integracji wdrażanych urządzeń z istniejącą infrastrukturą Zamawiającego w tym wykonania niezbędnych konfiguracji zapewniających prawidłową współpracę nowych elementów z istniejącą siecią. Opracowanie dokumentacji powdrożeniowej: • schemat logiczny i fizyczny wdrożonej infrastruktury, • opis zastosowanej segmentacji IT/OT, • wykaz urządzeń wraz z ich lokalizacją i adresacją, • konfigurację VLAN, interfejsów, routingu i reguł bezpieczeństwa, • opis reguł komunikacji pomiędzy segmentami IT i OT, • dokumentację konfiguracji urządzeń UTM i przełączników,
Ilość	1 szt.

24. Oprogramowanie typu NDR (Network Detection & Response)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Oprogramowanie NDR wraz dedykowana 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: I. Wykrywanie i reagowanie: o Ocena ryzyka, o Zarządzanie ryzykiem, o Analiza zagrożeń, o Polityki informowania o ryzyku, o Pułapki na cyberataki, o Wykluczenia, o Monitorowanie portów,

	o Powiadomienia o zdarzeniach, o Nadawca dziennika, o Kwarantanna, o Reguły ochrony, II. Zarządzanie siecią: o Obsługa ramek Jumbo, o Obsługa VLAN, o Konfiguracja IP, III. Przestrzeń dyskowa: o Pojemność systemu, o Wolumin aplikacji, o Typ RAID, o Informację o dysku i informacje SMART, o Test SMART dysku i harmonogram testu SMART, o Skanowanie I odzyskiwanie uszkodzonych bloków na dysku, IV. Zarządzanie dziennikami: o Dziennik zdarzeń, o Dziennik dostępu, o Użytkownicy online, o Ustawienia wpisów dziennika, o Ustawienia czasu przechowywania dziennika, o Ustawienia języka dziennika, o Nadawca dziennika, o Odbiorca dziennika, V. Monitor zasobów: o Zasoby systemowe- procesor/pamięć/sieć, o Zasoby pamięci masowej, o Wykorzystywanie woluminów/stanu/pamięci masowej, o Aktywność procesów. VI. Zabezpieczenia: o Certyfikat i klucz prywatny, o Wymiana certyfikatu i pobieranie certyfikatu, o Zasady dotyczące haseł, o Reguła siły hasła, o Reguła okresowej zmiany hasła, o Ochrona systemu przed manipulacjami, o Kontrola bezpieczeństwa. VII. Zarządzanie systemem: o Ustawienia ogólne, o Sprzęt, o Zasilanie, o Aktualizacja systemu, o Kopia zapasowa/przywracanie,

	o UPS, o Status systemu, o Uprawienia, o Zarządzanie użytkownikami, o Serwer SSH, o Usługa SNMP (V1/V2/V3) o Usługa wykruwania UPnP VIII. Obsługiwane klienckie systemy operacyjne: o Apple Mac OS 10.7 o Linux o Unix, o Microsoft Windows 7, 8, 10, 11 lub nowsze, o Microsoft Windows Server 2003, 2008 R2, 2012, 2012 R2, 2016, 2022 lub nowsze IX. Wspierane przeglądarki: o Apple Safari 7 lub nowsze, o Google Chrome, o Microsoft Internet Explorer 10 lub nowsze, o Mozilla Firefox,
Specyfikacja techniczna platformy	System NDR musi zostać dostarczony na dedykowanej platformie 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 2 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: o IEEE 802.3u 100Tx Fast Ethernet o IEEE 802.3ab 1000BASE-T Gigabit Ethernet

	o IEEE 802.3bz 2.5G/5G BASE-T Multi-Gig Ethernet o IEEE 802.3an 10GBASE-T 10G Ethernet o IEEE 802.3ae 10GBASE-SR o IEEE 802.3ae 10GBASE-LR o IEEE 802.3z 1000Base-X o IEEE 802.3x Kontrola przepływu w pełnym dupleksie o IEEE 802.1q Wirtualne sieci LAN (VLAN) o IEEE 802.1p Protokół QoS dla priorytetyzacji ruchu 18. Obudowa: Rack, maksymalnie 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 operacyjne	System musi mieć możliwość zainstalowania jednocześnie dwóch systemów 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	Minimum 12 miesięcy gwarancji producenta
Ilość	1 szt.

IV. OBSZAR KOMPETENCYJNY

25. Dostęp do platformy edukacyjnej z zakresu cyberbezpieczeństwa dla pracowników w celu regularnego podnoszenia świadomości i SZBI (IT/OT)

Nazwa	Minimalne wymagania dla sprzętu
Typ	Dostęp do platformy edukacyjnej z zakresu cyberbezpieczeństwa dla pracowników w celu regularnego podnoszenia świadomości i SZBI (IT/OT).
Wymagania ogólne	Platforma szkoleniowe typu security awerness. Platforma dostarczająca narzędzia i zasoby niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami. Użytkownicy mają otrzymać dostęp

	do materiałów szkoleniowych oraz testów wiedzy. Menedżerowie grup oraz administratorzy mają otrzymać wgląd w postęp nauki i poziom wiedzy w całej organizacji i dla poszczególnych grup.
Wymagania szczegółowe	Platforma musi zawierać minimum: • Materiały szkoleniowe podzielone na min 12 modułów w minimum 65 lekcjach • Minimum 17 testów wiedzy • Statystyki i raporty dla użytkowników, grup i menadżerów. Każdy moduł składać się ma z min z 4-7 lekcji w formie video oraz testu. Oprócz testów wewnątrz modułu, kurs musi zawierać również testy obejmujące swoim zakresem tematycznym przekrojowo więcej niż 1 moduł szkoleniowy. Szkolenie musi zostać przygotowane i odpowiednio ułożone przez ekspertów w dziedzinie cyberbezpieczeństwa, a informacje w nim zawarte muszą być aktualne, istotne i odnoszące się do realnych zagrożeń, na które użytkownik może natknąć się podczas codziennego korzystania z komputera. Zakres tematyki w zakresie minimum: • Socjotechniki • Bezpieczeństwo haseł • Bezpieczeństwo poczty e-mail i ochrona przed SCAM-em • Obrona przed phishingiem • Bezpieczeństwo stron WWW i przeglądarek • Ataki socjotechniczne z wykorzystaniem urządzeń • Ataki za pośrednictwem telefonu • Zagrożenia związane w urządzeniami mobilnymi • Zagrożenia związane z sieciami Wi-Fi • Zagrożenia w mediach społecznościowych • Dobre praktyki bezpieczeństwa • Prywatność, poufność i anonimowość w Internecie Cechy szkolenia: • Umożliwia monitorowanie postępu użytkownika • Statusy lekcji: nierozpoczęta, w toku, ukończona • Statusy modułu: nierozpoczęty, w toku, ukończony • Statusy testu: nierozpoczęty, rozpoczęty, niezaliczony, zaliczony • Brak ustalonej kolejności kursu, użytkownik może od razu przejść do zaliczenia testu lub zapoznawać się z lekcjami video według uznania lub według narzuconego w organizacji harmonogramu • Każdy moduł zawiera krótkie streszczenie zawartości • Każda lekcja zawiera notatki w formie tekstowej • Po ukończeniu materiału użytkownik wciąż ma do niego nieograniczony dostęp w ramach trwającej subskrypcji, przypisanej do organizacji

	• Postęp w lekcji jest zapisywany, użytkownik po powrocie do danej lekcji zaczyna od momentu, w którym zakończył oglądanie materiału video • Kurs umożliwia filtrowanie dostępnych modułów kursu (wszystkie moduły, nowe, rozpoczęte, ukończone) • Kurs pozwala użytkownikowi na ukrywanie ukończonych lekcji • Po ukończeniu kursu użytkownik otrzymuje certyfikat (do wydruku) • Administrator platformy ma możliwość konfigurowania minimalnego postępu w kursie (tempa postępów) osiąganego przez użytkowników • Szkolenie dostępne również w wersji mobilnej z poziomu przeglądarki, bez konieczności instalacji dodatkowego oprogramowania Test: • Musi składać się z pytań i odpowiedzi jednokrotnego wyboru • Do testu można podejść przed ukończeniem lekcji video (dowolna kolejność wykonywania działań w obrębie kursu) • Administrator platformy musi mieć możliwość konfigurowania progu punktowego wymagan • Administrator platformy ma możliwość konfigurowania czasu, który musi upłynąć zanim • Użytkownik po raz kolejny może podejść do testu • Test zapamiętuje odpowiedzi użytkownika (na wypadek opuszczenia testu przed ukończeniem) • Kolejność pytań i odpowiedzi jest losowana przed rozpoczęciem przez użytkownika testu • Ukończenie/Zaliczenie testu wpływa na postęp ukończenia modułu • Brak limitu czasowego na ukończenie testu • Zmiana wymaganego w organizacji progu procentowego zaliczenia testu po ukończeniu przez użytkownika testu nie ma wpływu na status testu (zaliczony/niezaliczony) • Kurs zawiera test końcowy sprawdzający wiedzę z całego kursu ego do zaliczenia testu Zarządzanie platformą: Zarządzanie użytkownikami: • Podział na 3 role: właściciel konta - Administrator Główny - z uprawnieniami administratora, administrator, użytkownik • Administrator Główny jest kontem zarządzającym platformą, zintegrowanym z zewnętrznym serwisem do zarządzania subskrypcją, który jest właścicielem subskrypcji. • Konto Administratora Głównego nie wlicza się do limitu użytkowników subskrypcji, ma dostęp do wszystkich funkcji platformy. Konta Administratora Głównego nie można usunąć, dezaktywować lub obniżyć uprawnień. Edycja danych Administratora Głównego wymaga zalogowania się do zewnętrznego serwisu do zarządzania subskrypcją

	• Administrator jest rolą nadawaną przez Administratora Głównego lub innego Administratora, ma dostęp do wszystkich funkcji platformy, można go usunąć, dezaktywować lub obniżyć uprawnienia • Użytkownik - ma dostęp do swojego pulpitu oraz szkolenia w platformie, nie może zarządzać platformą. Konto użytkownika może zostać utworzone ręcznie przez dowolnego administratora lub zaimportowanie z pliku .CSV. • Możliwość nadania funkcji menedżera grupy - wiąże się z rozszerzeniem widoczności użytkownika o członków grupy, którymi zarządza (wglądu do ich danych, postępów w nauce itd.) • Platforma pozwala na śledzenie postępów użytkowników w kursie (tylko dla Administratorów oraz Menedżerów) • Platforma wyświetla listę aktywności każdego użytkownika w organizacji wraz z informacją o dacie i rodzaju aktywności Właściwości użytkowników: • Imię i nazwisko, e-mail oraz rola (administrator/użytkownik) • Wymóg unikalnego adresu e-mail w obrębie organizacji • Możliwość dodawania użytkowników do platformy z poziomu interfejsu (formularz) • Możliwość masowego dodawania użytkowników oraz grup do platformy poprzez import pliku .json. • Możliwość masowego dodawania użytkowników do platformy poprzez import pliku csv • Możliwość aktualizacji danych użytkownika (imię i nazwisko) za pomocą importu csv. • Importowany plik może mieć do 5000 wierszy (limit użytkowników) • Po dodaniu użytkownika do platformy, otrzymuje on wiadomość e-mail z zaproszeniem do organizacji i ustaleniem pierwszego hasła • Administrator może dowolnie edytować dane wszystkich użytkowników (imię, nazwisko, adres e-mail, rola) • Administrator może dowolnie aktywować oraz dezaktywować konta wszystkich użytkowników • Administrator może dowolnie usuwać konta wszystkich użytkowników • Administrator ma dostęp do wszystkich funkcji w platformie • Administrator ma dostęp do wszystkich zakładek w platformie • Użytkownik ma dostęp do zakładki „Pulpit" oraz „Mój kurs" • Menedżer ma rozszerzony dostęp do grup i użytkowników, którymi zarządza
Licencjonowanie	Platforma musi być udostępniana w formie płatnego dostępu do usługi on-line w chmurze. Zamawiający wymaga dostępu dla minimum 40 pracowników do platformy do dnia 31.12.2026 r.
Ilość	1 szt.

26. Szkolenie dotyczące cyberbezpieczeństwa i cyberhigieny dla pracowników, działu IT oraz kadry zarządzającej

Nazwa	Minimalne wymagania dla sprzętu
Typ	kolenie dotyczące cyberbezpieczeństwa i cyberhigieny dla pracowników, działu IT oraz dry zarządzającej poprzedzone symulowanymi atakiem phishingowym (IT/OT)
Szkolenie socjotechniczne phishing	ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do zeprowadzenia 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: o opis wykorzystanych i skonfigurowanych domen o opis szablonów oraz opis celu jaki stanowił podczas realizacji kampanii o opis niebezpieczeństw związanych z dalszymi krokami prawdziwego ataku o statystyki kampanii phishingowej, w tym: liczby wysłanych, otwartych maili, liczby kliknięć w link, liczby osób, które podały swoje dane podsumowanie oraz rekomendacje.
Szkolenie cyberbezpieczeństwa	kolenie musi zostać przeprowadzone w maksymalnie dwóch grupach liczących aksymalnie 20 osób. kolenie dla każdej grupy musi trwać minimum 1 godzinę. Szkolenie musi obejmować w kresie 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	mawiający wymaga, aby szkolenia dedykowane dla pracowników jednostki rganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających

	wiadomość cyberzagrożeń.
Ilość	1 szt.