Fundusze Europejskie

na Rozwój Cyfrowy

ZAŁĄCZNIK NR 1

Opis Przedmiotu Zamówienia

Oprogramowanie oraz infrastruktura sprzętowa

SPIS TREŚCI

Wstęp

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Świebodzin realizowanego w ramach „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.

I. WYMAGANIA OGÓLNE

1. RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ

1) 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) 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: "Zainstalowane dwa procesory min. 16-rdzeniowe klasy x86, min. 2.5GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 330 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej" należy rozumieć jako:
"Zainstalowane co najmniej dwa procesory, posiadające co najmniej 16 rdzeni, klasy co najmniej x86, posiadające taktowanie co najmniej 2.5GHz, umożliwiające osiągnięcie wyniku co najmniej 330 w teście SPACrate2017_int_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej".

II. Obszar techniczny

Serwer

Nazwa	Minimalne wymagania dla sprzętu
Typ	Serwer (sprzęt serwerowy do klastra wraz z niezbędnym oprogramowaniem) dla Urzędu Gminy w Świebodzinie
Obudowa	• Obudowa Rack o wysokości max 2U • Obudowa wyposażona w min. 8 zatok na dyski 2.5” • Obsługa dysków SAS/SATA/NVMe • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. • 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 do dwóch procesorów. • Obsługa procesorów min. 56 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera • Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane minimum dwa procesory min. 16-rdzeniowe klasy x86, min. 2.5GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 330 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	Minimum 512GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający • Min. 8GB nieulotnej pamięci cache, • Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. • Wsparcie dla dysków samoszyfrujących
Dyski twarde	• Zainstalowane min.: ○ 2x dysk SSD SATA o pojemności min. 960GB, 12Gb, Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	Min. osiem slotów PCIe
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	• Min. 4 porty USB w tym min: o 1 port USB 3.0 z tyłu obudowy, o 1 port micro USB z przodu obudowy • Min. 2 porty VGA z czego jeden z przodu obudowy • Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W 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
System operacyjny/dodatkowe oprogramowanie	Licencja musi uprawniać do uruchamiania Serwerowego Systemu Operacyjnego (SSO) w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Serwerowy System Operacyjny (SSO) musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

	11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Graficzny interfejs użytkownika. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. 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. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. 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. f. Szyfrowanie plików i folderów.

	g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, l. 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 – Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. – Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) 23. 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. 24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 27. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
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 równoważnymi. 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 dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 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 WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym

	o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
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.
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. ○ 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 ○ 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 ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania

	○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ 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, ○ 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 ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ 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. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ 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 ○ 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 ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

	• Certyfikaty
	  ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:
	  ▪ ISO 27001 lub równoważny
	  ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization lub równoważny
	  ▪ CSA Cloud Control Matrix lub równoważny

Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub normami równoważnymi • Serwer musi posiadać deklaracja CE lub równoważną. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
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 na okres min. 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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 od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, 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: ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ 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. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub normy równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Wdrożenie	W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług: • Konfiguracja serwera: ○ stworzenie planu wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie serwera wirtualizacyjnego w wskazanej przez Zamawiającego szafie rack. ○ montażu w/w sprzętu w dostarczanej szafie rack w sposób zgodny z zaleceniami producenta dostarczanych serwerów. Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera.

	○ podłączenia serwera do wskazanej przez Zamawiającego infrastruktury sieciowej za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera ○ Instalacja system operacyjnego, konfiguracja dostarczonych serwerów w klaser wysokiej dostępności ○ podłączenie dostarczonej macierzy dyskowej do serwerów, skonfigurowanie i udostepnienie uzyskanej przestrzeni dyskowej ○ wykonać testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania. • Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska serwerowego. • Wymaga się, aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta. • Wymaga się, aby Wykonawca w ramach dostawy serwera zapewnił dostęp do urządzenia kryptograficznego spełniającego wymagania FIPS-140 Level minimum 3. Urządzenie to może być dostępne dla Zamawiającego jako urządzenie w Cloud z gwarancją przechowywania kluczy kryptograficznych na terenie Polski, lub jako osobne urządzenie w formie karty PCIe lub osobnego urządzenia dostępnego z poziomu sieci LAN. • Na potrzeby udostępnienia takiej usługi Wykonawca musi zapewnić osobny slot urządzenia kryptograficznego na wyłączne potrzeby Zamawiającego. Wymagane interfejsy komunikacji z urządzeniem kryptograficznym PKCS#11, CSP/CNG. Komunikacja sieciowa pomiędzy siedzibą Zamawiającego a urządzeniem kryptograficznym musi być zaszyfrowana za pomocą połączenia IPSEC z kluczem szyfrującym o długości minimum 256bitów typu AES. Dopuszczalne jest użycie algorytmu ECC o długości 192bitów.
Ilość	2 szt.

Macierz dyskowa

Nazwa	Minimalne wymagania dla sprzętu
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5”
Przestrzeń dyskowa	Zainstalowane: Min. 10x dysk SSD SAS o pojemności min. 3.84TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.

Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)
Kable/wkładki	Min. 4x kabel DAC 25GbE SFP28/SFP28 min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).

	Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Vmware. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek.

	Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Certyfikaty	Urządzenie musi spełniać następujące standardy bezpieczeństwa: • EN 62368-1 (European Union) lub równoważne • IEC 60950-1 (International) lub równoważne Dodatkowo musi być produkowany zgodnie z normami: • ISO 9001 oraz ISO 14001 lub równoważnymi Oraz posiadać deklaracja zgodności CE lub równoważna
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: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.

	○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ 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. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ 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. ○ 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 ○ 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.

	○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ 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 ○ 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 ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 lub równoważna ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization lub równoważna ▪ CSA Cloud Control Matrix lub równoważna
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta na okres min. 36 miesięcy Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia

	pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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 od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, 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: • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. • 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. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

	Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Wdrożenie	• Zamawiający wymaga, aby wykonawca wykonał następujące prace wdrożeniowe: Instalacja fizyczna sprzętu w serwerowi. • Ustawienie adresacji i podłączenie urządzeń zgodnie z wymaganiami Zamawiającego. • Aktualizacja oprogramowania systemowego oraz układowego wdrażanych rozwiązań do najnowszego na dzień wdrożenia • Skonfigurowanie macierzy dyskowej RAID 6 (z uwzględnieniem 1 dysku hotspare), przydzielenie przestrzeni dyskowej zgodnie z wymaganiami Zamawiającego dla zasobów macierzy, konfiguracja usług snapshot i clone. • Przygotowanie dokumentacji powdrożeniowej.
Ilość	1 szt.

UPS

Nazwa	Minimalne wymagania dla sprzętu
Typ	UPS dla Urzędu Gminy w Świebodzinie
Minimalne wymagania techniczne dla jednostki UPS	Moc znamionowa jednostki nie mniej niż 3000VA / 2700W Możliwość zastosowania w wersji wolnostojącej i do montażu w Rack Technologia Podwójnej konwersji (online) Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Wysokość n.p.m. podczas pracy 0-3000 m • Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55,0 dBA • Rozpraszanie ciepła w trybie online 703,00 BTU/h Sprawność: • Praca on-line ≥ 93,5% przy pełnym obciążeniu • Klasa ochrony IP 20 • Klasa energetyczna sprzętu przeciwprzepięciowego 340J • automatyczne włączenie UPS-a po powrocie zasilania • możliwość zimnego startu • tryb ECO
Parametry wejściowe	• Nominalne napięcie wejściowe 220, 230, 240V • Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne) • Typ gniazda wejściowego: IEC-320 C20, • Zmienny zakres napięcia wejściowego w trybie podstawowym 100 – 275V
Parametry wyjściowe	• Napięcie wyjściowe 220, 230, 240V • Częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz (±3Hz dla zasilania z sieci lub ±0.1Hz dla zasilania z baterii) • Współczynnik szczytu 3: 1 • Typ przebiegu sinusoida

	• Złącza/gniazda wyjściowe Minimum 8 szt. IEC 320 C13 (Zasilanie gwarantowane) Minimum 2 szt. IEC 320 C19 (Zasilanie gwarantowane) • Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny • Czas autonomii: minimum 20 minut dla pełnego obciążenia Minimum 46 minut dla połowy obciążenia • Typowy czas ładowania minimum 3 godziny • Oczekiwana żywotność akumulatora (lata) minimum 3 • Baterie wymieniane na gorąco • Możliwość rozszerzenia czasu podtrzymania poprzez dodanie do minimum 10 zewnętrznych pakietów akumulatorowych • Baterie wymieniane na gorąco • Automatyczny test akumulatora
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 (Zasilacz dostarczany wraz z kartą zarządzania sieciowego oraz czujnikiem temperatury) • Porty komunikacyjne: RJ-45, Smart-Slot, USB • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Awaryjny wyłącznik zasilania (EPO)
Certyfikaty, zgodności oraz gwarancja	• C, CE, EAC, RoHS, REACh lub równoważne • Min. 36 miesięcy gwarancji producenta naprawy lub wymiany urządzenia (bez akumulatora) i min. 24 miesiące na akumulatory.
Wdrożenie	• Konfiguracja i integracja z dostarczanym serwerem i macierzą dyskową czas pracy na podtrzymaniu bateryjnym i akcji wyłączenia po min. min. 10 minutach pracy na podtrzymaniu bateryjnym.
Ilość	1 szt.

Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X dla Urzędu Gminy w Świebodzinie
Wymagania ogólne	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
Parametry fizyczne platformy	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.

	• Zasilanie AC 230V. • Maksymalny pobór mocy: 30 W. • Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe - wymagania minimalne	Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości min.: • 24 porty GE RJ-45 • 4 porty 10 GE SFP+
Zarządzanie	• Wbudowany min. 1 port konsoli szeregowej do pełnego zarządzania. • Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	• Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
Funkcje urządzenia przy integracji z systemem	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.

centralnego zarządzania lub bezpieczeństwa	• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min. do 30.06.2026, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Ilość	1 szt.

Punkt dostępowy WiFi

Nazwa	Minimalne wymagania dla sprzętu
Typ	Punkt dostępowy WiFi (urządzenie AP) dla Urzędu Gminy w Świebodzinie
Wymagania ogólne	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: • Temperatura 0–50°C, • Wilgotność 5–90%. 2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington. 3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: • 2.4 GHz lub 5.0 GHz a/b/g/n/ac/ax, • 5.0 GHz a/n/ac/ax, • 2.4 GHz service b/g/n/ax 4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. 5. Urządzenie musi być wyposażone w moduł BLE/ZigBee. 6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 10/100/1000 Base-TX oraz interfejs konfiguracyjny RS-232 RJ45. 7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: • Tunnel, • Bridge, • Mesh. 9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist,

	802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA). 11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje: a. MIMO – 2x2, b. Maksymalna przepustowość dla poszczególnych modułów radiowych: i. 1201 Mbps; ii. 1201 Mbps; iii. 574 Mbps. c. Wymagana moc nadawania: i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; ii. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; d. Wsparcie dla 802.11n 20/40Mhz HT, e. Wsparcie dla kanałów 80MHz, f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 3.5dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz. g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, h. Maksymalna deklarowana liczba klientów per moduł radiowy: i. 512; ii. 512; iii. 512. 12. Funkcje dodatkowe: • OFDMA • Spatial Reuse (BSS Coloring) • UL-MU-MIMO 802.11ax • DL-MU-MIMO • Enhanced Target Wake Time (TWT)
Gwarancja	Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do minimum 60 miesięcy od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres do 30.06.2026, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Ilość	2 szt.

Oprogramowanie typu EDR Endpoint Detection and Response

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie typu EDR Endpoint Detection and Response dla Gminy Świebodzin
Wymagania ogólne	W ramach dostawy Zamawiający wymaga dostarczenia wznowienia aktualnie posiadanej licencji na oprogramowanie antywirusowe ESET PROTECT Advanced (obejmującej 140 stanowisk). Dodatkowo w ramach realizacji przedmiotu zamówienia,

	Zamawiający wymaga podniesienia funkcjonalności posiadanej licencji do rozwiązania klasy EDR. Dostarczone licencje muszą być ważne do 30-06-2026. Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo: - wdrożenia - skonfigurowania dla wszystkich użytkowników - przeszkolenia administratorów dostarczonego oprogramowania, wg ustaleń z Zamawiającym.
OPIS RÓWNOWAŻNOŚCI – wymagania minimalne:	
Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. 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/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11) posiadane przez Zamawiającego. 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

	5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać 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). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać 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 heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. 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. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i

	sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. 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. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, 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 możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V posiadanego przez Zamawiającego. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. 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.
Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem. 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 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 skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:

	a) Czysty, b) Podejrzany, c) Bardzo podejrzany, d) Szkodliwy. 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia
Moduł XDR	1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików

	wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Wymagania dodatkowe	Zamawiający wymaga, aby Wykonawca dokonał wdrożenia proponowanego rozwiązania. W ramach wdrożenia rozwiązania zamawiający wymaga w zakresie minimum: - Instalacja serwera konsoli EDR na maszynie wskazanej przez Zamawiającego; - Wstępna konfuguracja; - Przygotowanie wstepnych, domyślnych polityk; - Wdrożenie agenta EDR - Sprawdzenie poprawności działania serwera konsoli EDR - Przegląd detekcji zgromadzonych w konsoli - Wspólna analiza i optymalizacja, - Wspólne tworzenie wykluczeń Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania.
Ilość	1 szt.

Oprogramowanie SIEM Security Information and Event Management

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do zarządzania logami SIEM/SOAR dla Urzędu Gminy Świebodzin.
Wymagania ogóle	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. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”. 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, f) 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: • zdefiniowanie daty końcowej, • bez daty końcowej, • określenie liczby raportów, 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: • ilość zdarzeń nowych i niesklasyfikowanych, • ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa, • ilość zdarzeń sklasyfikowanych jako fałszywe alarmy, b) wykres przedstawiający skale zagrożeń, który uwzględnia: • ilość zasobów krytycznych na których są obsługiwane zdarzenia, • ilość zasobów niekrytycznych na których są obsługiwane zdarzenia, c) wykres przedstawiający źródła zagrożeń, który uwzględnia: • ilość nowych zdarzeń dotyczących użytkowników, • ilość podjętych zdarzeń dotyczących użytkowników, • ilość nowych zdarzeń dotyczących zasobów, • ilość podjętych zdarzeń dotyczących zasobów, d) wykres przedstawiający poziom zagrożeń, który uwzględnia: • ilość nowych zdarzeń w podziale na priorytety, • ilość podjętych zdarzeń w podziale na priorytety, e) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia: • ilość zdarzeń zarejestrowanych w bieżącym dniu, • ilość zdarzeń zarejestrowanych w ostatnim tygodniu, • ilość zdarzeń zarejestrowanych w ostatnim miesiącu, • ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu, f) wykres przedstawiający zagrożone usługi, który uwzględnia:

	• ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, • ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia, g) wykres przedstawiający zagrożone dane, który uwzględnia: • ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, • ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, h) wykres przedstawiający skale podatności, który uwzględnia: • ilość zasobów krytycznych na których są obsługiwane podatności, • ilość zasobów niekrytycznych na których są obsługiwane podatności, i) wykres przedstawiający czas obsługi podatności, który uwzględnia: • ilość podatności zarejestrowanych w bieżącym dniu, • ilość podatności zarejestrowanych w ostatnim tygodniu, • ilość podatności zarejestrowanych w ostatnim miesiącu, • ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu, j) wykres przedstawiający wagę podatności, który uwzględnia: • ilość nowych podatności w podziale na priorytety, • ilość podjętych podatności w podziale na priorytety, 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 zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). 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 min 200 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 do 30.06.2026roku. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego). Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu. Wykonawca w ramach dostawy musi zapewnić bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 2 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez Certyfikowanego Inżyniera systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.
Wymagania dodatkowe	Proces wdrożenia systemu powinien zostać przeprowadzony w porozumieniu z Zamawiającym. Wymagane jest podłączenie wszystkich źródeł logów wskazanych przez Zamawiającego do górnej granicy dostarczanych licencji. Należy uruchomić wszystkie niezbędne funkcjonalności umożliwiające korelację zdarzeń i logów z podłączonych źródeł. W ramach wdrożenia rozwiązania SIEM Zamawiający wymaga, aby Wykonawca wdrożył rozwiązanie SIEM na minimum 2 maszynach wirtualnych przygotowanych

	przez Zamawiającego. Wymaga się, aby Wykonawca przygotował harmonogram wdrożenia uwzględniający 4 etapy wdrożenia. 1etap - Analiza przedwdrożeniowa, 2 etap - Instalacja systemu, 3 etap - konfiguracja systemu, 4 etap - dostrojenie systemu, Zamawiający wymaga wdrożenia kompletnego systemu, w ramach którego zostanie podłączonych do 200 źródeł logów z systemów takich jak serwery fizyczne, serwery wirtualne, urządzenia sieciowe, rozwiązania endpoint protection takie jak AV, systemów backupu. W ramach etapu 1 wymaga się przygotowania przeprowadzenia analizy zmierzającej do określenia istotnych informacji które SIEM powinien wykrywać z podłączonych źródeł logów w ramach swojego monitoringu. Analiza ma na celu przygotowanie do stworzenia dedykowanych reguł bezpieczeństwa i ich implementacji na etapie konfiguracji systemu. W etapie 2 Wykonawca musi zainstalować zaoferowane oprogramowanie według wcześniej przedstawionej architektury działania rozwiązania oraz wcześniej przygotowanego schematu komunikacji sieciowej w sieci lokalnej Zamawiającego. Na etapie 3 Wykonawca musi zaimplementować wcześniej opracowanie reguły bezpieczeństwa wraz z weryfikacją ich działania dla konkretnych procesów określonych na etapie analizy przedwdrożeniowej. Etap 4 musi zawierać dostrojenie systemu tak aby nie powodował nadmiernej ilości fałszywych alarmów zaciemniających realne możliwe zagrożenia. Nie dopuszcza się sytuacji, w której jedno źródło logów spowoduję destabilizację działania całego systemu SIEM w krótkim okresie czasu np. 10minut.
Ilość	1 szt.

Oprogramowanie do zdalnego dostępu

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do zdalnego dostępu dla Urzędu Gminy w Świebodzinie
Wymagania ogólne	Zamawiający wymaga dostarczenia licencji oprogramowania do zdalnego dostępu na okres do 30.06.2026 o parametrach minimalnych: • Min. 2 połączenia jednoczesne • Możliwość połączenia się z nieograniczoną liczbą urządzeń • Do 1000 zarządzanych urządzeń (dostęp nienadzorowany) • Interfejs linii poleceń • Masowe wdrożenie (MSI) • Obsługa urządzeń mobilnych
Ilość	1 szt.

III. Obszar kompetencyjny

Szkolenia dla działu IT typ 1

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 1 dla Gminy Świebodzin
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 5 dni) dla administratora Zamawiającego (1 osoba) z zakresu administrowania systemami operacyjnymi serwera. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym.
Wymagania szczegółowe	Program szkolenia będzie obejmować w zakresie minimum: 1. **Instalacja, aktualizacja i migracja serwerów i obciążeń** • Przedstawiamy systemie operacyjnym • Przygotowanie i instalacja Server Core • Przygotowanie do aktualizacji i migracji • Migracja ról i obciążeń serwera • Modele aktywacji systemu operacyjnego 3. **Konfiguracja pamięci lokalnej** • Zarządzanie dyskami w systemie operacyjnym • Zarządzanie wolumenami w systemie operacyjnym • Tworzenie i zarządzanie wolumenami • Zmiana rozmiaru woluminów • Zarządzanie wirtualnymi dyskami twardymi 4. **Wdrażanie rozwiązań pamięci masowej dla przedsiębiorstw** • Przegląd rozwiązań DAS, NAS i SAN • Porównanie Fibre Channel, iSCSI i Fibre Channel przez Ethernet • Zrozumienie iSNS, DCB i MPIO • Konfiguracja udostępniania w Windows Server • Planowanie wymagań magazynowych • Konfiguracja pamięci iSCSI • Konfiguracja i zarządzanie infrastrukturą współdzieloną 5. **Wdrażanie przestrzeni dyskowych i deduplikacji danych** • Wdrażanie przestrzeni dyskowych • Zarządzanie przestrzeniami do przechowywania • Wdrażanie deduplikacji danych • Tworzenie miejsca do przechowywania • Instalowanie deduplikacji danych • Konfigurowanie deduplikacji danych

	6. **Instalacja i konfiguracja Hyper-V i maszyn wirtualnych** • Przegląd witalizatora • Instalowanie witalizatora • Konfigurowanie magazynu na serwerach hosta witalizatora • Konfigurowanie sieci na serwerach hosta witalizatora • Konfigurowanie maszyn wirtualnych witalizatora • Zarządzanie maszynami wirtualnymi • Konfiguracja sieci witalizatora • Konfiguracja maszyn wirtualnych • Zagnieżdżona wirtualizację dla maszyny wirtualnej 7. **Wdrażanie i zarządzanie kontenerami** • Przegląd kontenerów w Windows Server • Wdrażanie kontenerów systemu operacyjnego i witalizatora • Instalowanie, konfigurowanie i zarządzanie kontenerami za pomocą Docker • Instalowanie i konfigurowanie kontenerów systemu operacyjnego za pomocą programu interpretatora poleceń • Wdrażanie kontenerów za pomocą Docker 8. **Wysoka dostępność i odzyskiwanie po awarii** • Definiowanie poziomów dostępności • Planowanie rozwiązań zapewniających wysoką dostępność i odtwarzanie po awarii za pomocą maszyn wirtualnych Hyper-V • Tworzenie kopii zapasowych i przywracanie przy użyciu funkcji Kopia zapasowa systemu Windows Server • Wysoka dostępność dzięki klastrom pracy awaryjnej w systemie Windows Server • Określanie odpowiedniego rozwiązania zapewniającego wysoką dostępność i odtwarzanie po awarii • Wdrażanie migracji pamięci • Konfigurowanie replik Hyper-V 9. **Implementacja klastrów pracy awaryjnej** • Planowanie klastra pracy awaryjnej • Tworzenie i konfigurowanie nowego klastra pracy awaryjnej • Utrzymanie klastra pracy awaryjnej • Rozwiązywanie problemów z klastrem pracy awaryjnej • Wdrażanie wysokiej dostępności z klastrowaniem typu stretch • Tworzenie klastra pracy awaryjnej • Weryfikowanie ustawień kworum i dodawanie węzła • Eksmisja węzła i weryfikacja ustawień kworum • Modyfikacja ustawień kworum • Weryfikacja wysokiej dostępności 10. **Implementacja klastrów pracy awaryjnej w systemie operacyjnym** • Omówienie integracji funkcji witalizatora z klastrami pracy awaryjnej • Wdrażanie maszyn wirtualnych witalizatora w klastrach pracy awaryjnej

	• Najważniejsze funkcje maszyn wirtualnych w środowisku klastrowym • Konfigurowanie klastra pracy awaryjnej dla witalizatora • Konfigurowanie maszyny wirtualnej o wysokiej dostępności 11. **Wdrażanie równoważenia obciążenia sieciowego** • Przegląd NLB • Konfigurowanie klastra równoważenia obciążenia sieciowego • Planowanie wdrożenia NLB • Wdrażanie klastra równoważenia obciążenia sieciowego (NLB) • Konfigurowanie i zarządzanie klastrem równoważenia obciążenia sieciowego • Weryfikowanie wysokiej dostępności klastra równoważenia obciążenia sieciowego 12. **Tworzenie i zarządzanie obrazami wdrożeniowymi** • Wprowadzenie do obrazów wdrożeniowych • Tworzenie i zarządzanie obrazami wdrożeniowymi za pomocą MDT • Środowiska maszyn wirtualnych dla różnych obciążeń • Konfiguracja MDT • Tworzenie i wdrażanie obrazu 13. **Zarządzanie, monitorowanie i konserwacja instalacji maszyn wirtualnych** • Omówienie programu WSUS i opcji wdrażania • Aktualizacja procesu zarządzania za pomocą WSUS • Omówienie Windows PowerShell DSC • Przegląd narzędzi do monitorowania systemu operacyjnego • Korzystanie z Monitora wydajności • Monitorowanie dzienników zdarzeń • Ustalenie punktu odniesienia wydajności • Identyfikacja źródła problemu z wydajnością • Przeglądanie i konfigurowanie scentralizowanych dzienników zdarzeń
Ilość	1 szt.

Szkolenia dla działu IT typ 2

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 2 dla Gminy Świebodzin
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 5 dni) dla administratora Zamawiającego (1 osoba) z zakresu administrowania bazami danych. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do 30.06.2026

Wymagania szczegółowe	Program szkolenia będzie obejmować w zakresie minimum: 1. Przygotowanie infrastruktury usługi katalogowej do zarządzania zasadami grupy. • Potrzeby organizacji w zakresie scentralizowanego zarządzania ustawieniami dla komputera i użytkownika. • Potrzeby organizacji w zakresie zapewnienia założonego poziomu bezpieczeństwa. • Infrastruktura usługi katalogowej. • Komponenty infrastruktury sieciowej. • Projektowanie infrastruktury jednostek organizacyjnych pod kątem efektywnego stosowania zasad grupy. 2.Wprowadzenie do interpretatora poleceń. • Wprowadzenie do interpretatora poleceń • Polecenia modułu GroupPolicy. • Dodatkowe moduły do zarządzania GPO • Skrypty logowania. • Zarządzanie zdalne 3.Wprowadzenie do zarządzania konfiguracją komputera i użytkownika. • Zarządzania konfiguracją. • Zarządzanie konfiguracją za pomocą zasad grupy. • Nowe funkcje zasad grupy wprowadzone w kolejnych wersjach systemu operacyjnego • Wykorzystanie interpretatora polceń w procesie zarządzania konfiguracją. 4.Narzędzia do zarządzania zasadami grupy. • Zasady lokalne i domenowe. • Konsola zarządzania zasadami grupy (GPMC). • Proces odświeżania GPO. • Konfiguracja zasad grupy do zdalnego zarządzania za pomocą Server Manager 5.Wprowadzenie do zarządzania i przetwarzania zasad grupy. • Uprawnienia do zarządzania obiektami zasad grupy. • Komponenty zasad grupy w Active Directory. • Proces przetwarzania zasad grupy. • Modyfikacja procesu przetwarzania zasad grupy. 6.Zapewnienie założonego poziomu zabezpieczeń za pomocą zasad grupy. • Komponenty architektury zabezpieczeń dla systemu operacyjnego.

	• Bezpieczeństwo konta użytkownika. • Polityka lokalna. • Zaawansowana inspekcja. • Hardening środowiska Windows • Zarządzanie certyfikatami za pomocą zasad grupy. • Analiza dziennika zabezpieczeń. 7.Zapewnienie bezpieczeństwa aplikacji za pomocą zasad grupy. • Zarządzanie ustawieniami UAC. • Ochrona przed złośliwym oprogramowaniem. • Wykorzystanie AppLocker do ograniczeń aplikacji. 8.Konfiguracja środowiska stacji roboczych. • Typy skryptów i kontrola ich wykonywania. • Ustawienia pulpitu, Menu Start oraz paska zadań. • Ustawienia panelu sterowania. • Zarządzanie drukarkami. • Ustawienia sieci. 9.Wirtualizacja stanu użytkownika. • Konfiguracja przekierowania folderów. • Zarządzanie plikami Offline. • Wdrożenie User Experience Virtualization. 10.Zarządzanie instalacją oprogramowania za pomocą zasad grupy. • Dystrybucja aplikacji za pomocą paczek MSI. • Punkty dystrybucyjne aplikacji. • Zarządzanie pakietami. 11.Szablony administracyjne. • Wprowadzenie do szablonów administracyjnych. • Zarządzanie szablonami ADMX. • Przygotowanie i zarządzanie Central Store. • Wdrażanie i zarządzanie oprogramowaniem Microsoft oraz firm trzecich za pomocą szablonów administracyjnych. 12.Preferencje zasad grupy. • Wprowadzenie do preferencji zasad grupy. • Porównanie preferencji i polityk grupowych.

	• Opcje konfiguracyjne preferencji. 13.Rozwiązywanie problemów i kopia zapasowa. • Narzędzia do rozwiązywania problemów. • Wynikowe zasady grupy (RSOP). • Podgląd zdarzeń. • Kopia zapasowa, przywracanie, importowanie i kopiowanie obiektów zasad grupy
Ilość	1 szt.

Szkolenia dla działu IT typ 3

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla pracowników działu IT typ 3 dla Urzędu Gminy
Szkolenie zakresu zarządzania i administracji oprogramowaniem do monitorowania infrastruktury informatycznej – wymagania minimalne	Zamawiający wymaga przeprowadzenia szkolenia z zakresu oprogramowania do monitorowania infrastruktury informatycznej, minimum dwudniowego (2), w formie stacjonarnej, prowadzonego przez certyfikowanego trenera. Najważniejsze funkcjonalności oprogramowania, Poprawna konfiguracja oprogramowania, Wymagania i instalacja systemu, Sposoby aktualizacji, Ćwiczenia praktyczne z wdrażania systemu, Monitoring krytycznych urządzeń w organizacji, Przeprowadzanie audytu oprogramowania i sprzętu, Monitorowanie aktywności użytkowników, Automatyzacja procesów obsługi zgłoszeń serwisowych, Zarządzanie nośnikami zewnętrznymi, Zarządzanie wskaźnikami aktywności pracowników.
Wymagania dodatkowe	Dodatkowo Zamawiający wymaga, aby uczestnik każdego szkolenia otrzymał: Materiały szkoleniowe w wersji elektronicznej Wsparcie poszkoleniowe trenera w okresie minimum 14 dni po zakończeniu szkolenia. Certyfikat ukończenia szkolenia
Ilość	1 szt.

Szkolenia dla działu IT typ 4

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 4 dla Urzędu Gminy
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 2 dni) dla administratora Zamawiającego (1 osoba) z posiadanego rozwiązania antywirusowego ESET.

	Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do 30.06.2026
Wymagania szczegółowe	• Program szkolenia będzie obejmować w zakresie minimum: • Omówienie dostępnych produktów, • Różnice pomiędzy konsolą ON-PREM a chmurową, • Różnice pomiędzy ochroną na poziomie antywirus i securit, • Przydatne strony WWW, • Konto administratora -zarządzanie licencjami (ćwiczenie), • Konsola do zarządzania - architektura i omówienie komponentów, • Instalacja i aktualizacja serwera z konsolą do zarządzania (ćwiczenie), • konsola - omówienie funkcji serwera, • Zarządzanie administratorami i ich uprawnieniami (ćwiczenie), • Zarządzanie agentami- zdalna instalacja i omówienie możliwości (ćwiczenie), • Grupy statyczne i dynamiczne, • Zadania klienta, serwera oraz wyzwalacze, • Zdalna instalacja klienta antywirusa, • Typowe scenariusze (ćwiczenia), • Omówienie funkcji podstawowych i zaawansowanych klienta, • Ochrona antywirusowa, • Zarządzanie aktualizacją, • Polityki i dziedziczenie (ćwiczenie), • Zapora osobista (ćwiczenie), • Typowe scenariusze (ćwiczenia), • Moduł antyspamowy, • Powiadomienia, • Raportowanie (ćwiczenie), • Kontrola dostępu do stron internetowych (ćwiczenie), • Kontrola dostępu do urządzeń (ćwiczenie), • Migracja konsoli lokalnej do konsoli chmurowej (ćwiczenie), • Wdrożenie klienta antywirusa na urządzenia z systemem Android (ćwiczenie), • Rozwiązywanie problemów. • Administrator po kursie otrzymuje zaświadczenia ukończenia szkolenia.
Ilość	1 szt.

Szkolenia dla działu IT typ 5

Nazwa	**Minimalne wymagania dla szkolenia**
Typ	Szkolenia dla działu IT typ 5 dla Gminy Świebodzin
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 1 dzień) dla administratora Zamawiającego (1 osoba) z posiadanego rozwiązania antywirusowego ESET. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym.

	Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do 30.06.2026
Wymagania szczegółowe	Program szkolenia będzie obejmować w zakresie minimum: • Utworzenie konta ESET Business Account i dodanie kluczy licencyjnych. • Wdrożenie i konfiguracja serwera centralnego zarządzania ESET PROTECT w postaci maszyny wirtualnej. • Migracja agentów ESET Management Agent pomiędzy serwerami. • Wdrożenie i konfiguracja usługi ESET Bridge w celu replikacji agentów przy pracy zdalnej oraz w środowiskach rozproszonych. • Zaawansowane zarządzanie politykami. • ESET Full Disk Encryption – szyfrowanie. • ESET LiveGuard Advanced – sandboxing chmurowy. • Rozwiązywanie problemów.
Ilość	1 szt.

Szkolenia dla działu IT typ 6

Nazwa	**Minimalne wymagania dla szkolenia**
Typ	Szkolenia dla działu IT typ 6 dla Gminy Świebodzin
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 1 dzień) dla administratora Zamawiającego (1 osoba) z posiadanego rozwiązania antywirusowego ESET. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do 30.06.2026
Wymagania szczegółowe	Program szkolenia będzie obejmować w zakresie minimum: 1. Wprowadzenie do tematu szyfrowania oraz przegląd produktów firmy ESET Endpoint Encryption. 2. Utworzenie środowiska centralnego zarządzania. 3. Omówienie interfejsu konsoli ESET Endpoint Enterprise Server. 4. Tworzenie użytkowników: a. integracja z Active Directory, b. ręczne tworzenie użytkowników, 5. Tworzenie paczek instalacyjnych: a. Ustawienie profilu paczki instalacyjnej, b. Ustawienie profilu stacji roboczej, 6. Zdalna instalacja klientów - szyfrowanie Full Disk Encryption 7. Omówienie interfejsu klienta ESET Endpoint Encryption Pro: a. szyfrowanie wiadomości e-mail, b. tworzenie zaszyfrowanych partycji wirtualnych, c. szyfrowanie nośników wymiennych (omówienie dostępnych metod szyfrowania), d. szyfrowanie plików i folderów, e. szyfrowanie tekstu, f. tworzenie archiwów samorozpakowujących, 8. Zdalna zmiana konfiguracji klientów

	9. Omówienie metod Recovery: a. przywracanie dostępu do systemu w przypadku zapomnienia hasła, b. tworzenie Emergency Disk.
Ilość	1 szt.

Szkolenia dla działu IT typ 7

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla działu IT typ 7 dla Gminy Świebodzin
Wymagania podstawowe	Wykonawca zapewni certyfikowane szkolenie (minimum 1 dzień) dla administratora Zamawiającego (1 osoba) z posiadanego rozwiązania antywirusowego ESET. Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie powinno zostać dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie do 30.06.2026
Wymagania szczegółowe	Program szkolenia będzie obejmować w zakresie minimum: • Omówienie pojęcia Extended Detection & Respond (XDR), • Architektura produktu ESET Inspect, • Wdrożenie serwera ESET Inspect (ćwiczenie), • Wdrożenie i konfiguracja agentów ESET Inspect (ćwiczenie), • Omówienie funkcji ESET Inspect, • Generowanie detekcji i ich analiza (ćwiczenie), • Reguły i automatyzacja (ćwiczenie), • Raportowanie, powiadomienia i zarządzanie uprawnieniami, • Rozwiązywanie problemów.
Ilość	1 szt.

Szkolenia dla pracowników spoza działu IT typ 8

Nazwa	Minimalne wymagania dla usługi
Typ	Szkolenia dla pracowników spoza działu IT typ 8
Wymagania ogólne	Szkolenie musi zostać przeprowadzone dla w min. 4 turach po min. 25 osób. Szkolenie powinno trwać minimum 1 h. Dopuszcza się szkolenie w formie zdalnej. Szkolenie musi obejmować w zakresie minimum: 1. Wycieki informacji – mechanizmy i skutki. 2. Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze. 3. Psychomanipulacja w sieci – zasady i zastosowania. 4. Sfałszowane komunikaty i strony – identyfikacja zagrożeń. 5. Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing) 6. Archiwizacja internetowa – cyfrowy ślad nie znika. 7. Mechanizmy śledzenia w sieci – rola i funkcja cookies. 8. Niebezpieczeństwa ze strony nieautoryzowanego sprzętu. 9. Ataki siłowe na hasła – jak nie dać się złamać. 10. Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing).

	11. Świadomość pracowników – kultura bezpieczeństwa w organizacji.
Ilość	1 szt.