Tekst alternatywny: u góry strony Logotyp Cyberbezpieczny samorząd, w stopce dokumentu umieszczono logotypy Funduszy Europejskich na rozwój cyfrowy, flagę Rzeczpospolitej Polskiej, Centrum Projektów Polska Cyfrowa i flaga Unii Europejskiej z informacją o dofinansowaniu

Nazwa zadania: „Gmina Niegowa cyberbezpiecznym samorządem" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC)

Załącznik nr 2 do SWZ – Szczegółowy Opis Przedmiotu Zamówienia

I. OPIS PRZEDMIOTU ZAMÓWIENIA

1. W ramach realizacji projektu „Cyberbezpieczny Samorząd" zaplanowano zakup urządzeń, oprogramowania, przeprowadzenia szeregu testów systemu teleinformatycznego i audytu wraz z wdrożeniem polityki bezpieczeństwa w budynku Urzędu Gminy Niegowa. Zaplanowano także szkolenia pracowników w zakresie cyberbezpieczeństwa.
2. Zakres realizacji zadania obejmuje:
   a. **Dostawę, uruchomienie i konfigurację serwera do backupu z systemem operacyjnym**, przeznaczonego do wykonywania kopii zapasowych systemów informatycznych oraz danych Urzędu Gminy Niegowa, zgodnie z zasadą ciągłości działania.
   b. **Dostawę oprogramowania do wykonywania kopii zapasowych (backup)** wraz z wdrożeniem i konfiguracją.
   c. **Dostawę dwóch (2) urządzeń klasy UTM** wraz z wdrożeniem, konfiguracją i implementacją polityk bezpieczeństwa zgodnie z wymaganiami użytkownika.
   d. **Dostawę trzech (3) przełączników zarządzalnych** wraz z konfiguracją i integracją z istniejącą infrastrukturą IT zgodnie z wymaganiami użytkownika.
   e. **Dostawę oprogramowania klasy SIEM** wraz z wdrożeniem i integracją z systemami Zamawiającego oraz szkoleniem z obsługi i konfiguracji.
   f. **Dostawę oprogramowania klasy EDR** wraz z wdrożeniem na stacjach roboczych i serwerach Zamawiającego oraz szkoleniem z obsługi i konfiguracji.
   g. **Przeprowadzenie audytu bezpieczeństwa systemów teleinformatycznych**, na podstawie którego Wykonawca opracuje oraz wdroży **Politykę Bezpieczeństwa Informacji** zgodnie z obowiązującymi przepisami.
   h. **Dostawę jednego (1) centralnego zasilacza awaryjnego UPS**, wraz z uruchomieniem i konfiguracją.
   i. **Dostawę i konfigurację urządzenia NAS**, przeznaczonego do archiwizacji systemów i danych, obsługującego minimum **45 użytkowników Urzędu Gminy Niegowa**, wraz z konfiguracją i archiwizacją.

Serwer do backupu, Oprogramowania do wykonywania kopii zapasowych

1) Urządzenie musi być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.

2) Nie dopuszcza się urządzenia posiadającego wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.

3) Elementy, z których zbudowane jest urządzenie muszą być produktami producenta urządzenia lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

4) Urządzenie musi być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.

5) Do urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim w formie papierowej lub elektronicznej.

6) Urządzenie na etapie dostawy pomiędzy producentem, a zamawiającym nie może podlegać modyfikacjom.

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	• Obudowa Rack o wysokości max 2U • 12 slotów na dyski 3.5” • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.3GHz (częstotliwość bazowa), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 200 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera.
RAM	• 128GB DDR5 RDIMM 6400MT/s,
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 ○ Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	• Zainstalowane: ○ 4x dysk SSD SATA o pojemności min. 1,92TB, Hot-Plug ○ 2x dysk HDD SATA o pojemności min. 4TB, 6Gb/s, 7,2tyś obr./min • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	• Trzy sloty PCIe
Interfejsy sieciowe/FC/SAS	• 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • 4 interfejsy sieciowe 2,5Gb Ethernet w standardzie BASE-T (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	• 4 portów USB w tym min: ○ 1 port USB 2.0 Type-C ○ 2 porty USB 3.1 ○ 1 port USB 3.0 wewnątrz obudowy • Port VGA z tyłu obudowy
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
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	• Fabrycznie zainstalowany system klasy np. Windows Server 2025 Standard lub równoważny

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	Przez system równoważny Zamawiający rozumie system operacyjny spełniający co najmniej następujące wymagania funkcjonalne i techniczne:a) Posiada natywne wsparcie dla wdrożonego u Zamawiającego środowiska katalogowego (Active Domain Services / LDAP) i umożliwia pełne zarządzanie uprawnieniami użytkowników, komputerów oraz polisami bezpieczeństwa (GPO lub równoważne).b) Posiada wbudowany, natywny hiperwizor (oprogramowanie do wirtualizacji typu Hypervisor) wspierający tworzenie i izolację maszyn wirtualnych z obsługą wirtualnego modułu bezpieczeństwa vTPM 2.0.c) Wspiera zaawansowane mechanizmy bezpieczeństwa, w tym: ochronę tożsamości poświadczeń (Credential Guard lub równoważne), szyfrowanie dysków i wolumenów (BitLocker lub równoważne) oraz integralność kodu opartej na wirtualizacji (VBS).d) Zapewnia natywną obsługę protokołów sieciowych SMB (w wersji min. 3.1.1) z wymuszaniem szyfrowania ruchu oraz obsługę protokołu TLS 1.3 dla zabezpieczenia komunikacji sieciowej.e) Producent systemu zapewnia dla oferowanej wersji pełne, oficjalne wsparcie techniczne oraz regularne, bezpłatne aktualizacje bezpieczeństwa (patche/poprawki) przez okres minimum 5 lat od momentu dostawy. • Dołączony przez producenta serwera nośnik • Nowa licencja pokrywająca wszystkie fizyczne rdzenie w serwerze • Menu, pomoc, komunikaty systemowe w jezyku polskim (zakres minimalny)
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 (wytyczne wskazano w certyfikacji)
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika o możliwość podmontowania zdalnych wirtualnych napędów o wirtualną konsolę z dostępem do myszy, klawiatury o wsparcie dla IPv6 o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer o integracja z Active Directory o możliwość obsługi przez sześciu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. ○ Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe możliwość rozszerzenia funkcjonalności o: ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i

	urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych ○ możliwość wykorzystania tokenu lub aplikacji do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej ○ Automatyczne odświeżanie certyfikatów SSL ○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ 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. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Spełnia normy ISO-9001 lub równoważną dla producenta sprzęt w zakresie produkcji • Spełnienia normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji • Posiada deklarację CE • Spełnia wymagania normy NIST SP 800-193 lub równoważnej w zakresie ochrony przed cyberatakami oraz być wyposażone w rozwiązania zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania zgodnie z wytycznymi NIST SP 800-147B i NIST SP 800-155 **Wykonawca wraz z ofertą złoży:** - **Oświadczenie producenta** oferowanego serwera potwierdzającego, że urządzenie w pełni spełnia wymagania i mechanizmy ochrony (Protection, Detection, Recovery) określone w normie NIST SP 800-193 - Lub **oryginalną dokumentację techniczną (np. whitepaper, specyfikacji technicznej, architektury bezpieczeństwa) wydanej przez producenta sprzętu**, z której wprost wynika wbudowana sprzętowa zgodność z wytycznymi normy NIST SP 800-193

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	- **LUB certyfikat niezależnej, akredytowanej jednostki badawczej** (np. TÜV, Kriterien, itp.), jeśli producent poddał urządzenie zewnętrznym testom na zgodność z tą publikacją • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest dokument pobrany ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku – **Wykonawca wraz z ofertą złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog ze statusem „Certified for Windows Server" dla wersji 2022 lub nowszej **lub na równoważnej publicznej liście kompatybilności innego systemu operacyjnego klasy Enterprise (np. Red Hat Ecosystem Catalog, VMware Compatibility Guide)**, zapewniającej analogiczne potwierdzenie stabilności, pełnego wsparcia technicznego producenta oprogramowania dla architektury sprzętowej oraz bezpieczeństwa przetwarzania danych
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	• Gwarancja producenta min. 5 lat • Możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i /lub przez Internet.

- Czas diagnostyki do 2 godzin od zgłoszenia

  Podjęcie zgłoszenia, rozpoczęcie zdalnej diagnostyki przez certyfikowanego inżyniera i przekazanie informacji zwrotnej do Zamawiającego o przyczynie usterki

- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.

- W przypadku **Awarii Krytycznej**, którą strony definiują jako błąd, usterkę lub uszkodzenie sprzętu/oprogramowania dostarczonego w ramach Umowy, które powoduje całkowite zatrzymanie pracy Urzędu, brak możliwości wykonywania kopii zapasowych, brak dostępu do kluczowych baz danych lub całkowitą przerwę w łączności sieciowej (brak działania firewall UTM), terminy kształtują się następująco :

Parametr SLA	Definicja	Maksymalny czas
Czas Reakcji (Diagostyka)	Podjęcie zgłoszenia, rozpoczęcie zdalnej diagnostyki przez certyfikowanego inżyniera i przekazanie informacji zwrotnej do Zamawiającego o przyczynie usterki.	**do 2 godzin** od zgłoszenia
Czas Obejścia (Tymczasowy)	Wdrożenie rozwiązania tymczasowego przywracającego kluczowe funkcje Urzędu, jeżeli ostateczna naprawa wymaga wymiany komponentów sprzętowych.	**do 8 godzin** od zgłoszenia
Czas Naprawy Ostatecznej	Pełne usunięcie awarii, wymiana uszkodzonych podzespołów na fabrycznie nowe lub regenerowane przez producenta i przywrócenie stanu pierwotnego.	**Następny Dzień Roboczy (Next Business Day)**

- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	• Firma serwisująca musi posiadać autoryzacje producenta urządzeń **– dokument należy załączyć do oferty.**

Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego.
- Na oferowanym urządzeniu musi zostać przeprowadzona aktualizacja firmware'u. Urządzenie zostanie skonfigurowane zgodnie z najlepszymi praktykami, a na serwerze zainstalowane zostanie oprogramowanie do wirtualizacji.

  Zamawiający wymaga dostarczenia i zainstalowania wraz z serwerem oprogramowania do wirtualizacji (typu Hypervisor działającego bezpośrednio na sprzęcie – Bare-Metal lub zintegrowanego z systemem operacyjnym klasy Enterprise) o architekturze 64-bitowej.Oferowane oprogramowanie musi wspierać natywną mikroarchitekturę procesorów serwera oraz posiadać funkcje sprzętowego wsparcia wirtualizacji (np. Intel VT-x lub AMD-V) oraz sprzętowego wsparcia dla translacji adresów stron pamięci (np. Intel EPT lub AMD NPT/RVI).Środowisko wirtualizacji musi umożliwiać uruchamianie systemów-gości (maszyn wirtualnych) z rodziny Windows Server oraz systemów Linux klasy Enterprise, zapewniając dla nich pełną integrację, dedykowane sterowniki optymalizujące wydajność (np. Integration Services) oraz wsparcie dla bezpiecznego rozruchu (Secure Boot).W celu zapewnienia najwyższego poziomu cyberbezpieczeństwa, oprogramowanie do wirtualizacji musi wspierać izolację maszyn wirtualnych na poziomie sprzętowym, obsługę wirtualnego modułu TPM (vTPM 2.0) dla maszyn wirtualnych oraz technologię ochrony pamięci RAM przed nieautoryzowanym odczytem.Zamawiający dopuszcza rozwiązanie zintegrowane z systemem operacyjnym serwera (np. Windows Server Hyper-V) lub dowolne oprogramowanie równoważne, które spełnia wszystkie powyższe wymagania techniczne, funkcjonalne i bezpieczeństwa, a także posiada publicznie dostępną i aktualną listę kompatybilności sprzętowej (HCL), na której znajduje się oferowany model serwera.
- W ramach wdrożenia, przy wykorzystaniu zaoferowanej licencji Microsoft Windows Server 2025 Standard (lub rozwiązania równoważnego), Wykonawca zobowiązany jest do konfiguracji środowiska wirtualizacji oraz utworzenia dwóch nowych maszyn wirtualnych z tym systemem operacyjnym, zgodnie z przysługującymi prawami do wirtualizacji dla tej licencji.
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Urządzenia klasy UTM

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 64 GB.
5. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 90 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.4 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.3 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.2 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox.
9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) **na okres 36 miesięcy**.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez **okres 36 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Rozszerzone wsparcie serwisowe AHB/SOS

System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora **przez okres 36 miesięcy**.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie urządzenia do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Wykonawca winien dysponować oświadczeniem producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym (dokument nie jest wymagany do złożenia na etapie postepowania przetargowego)

Przełączniki zarządzalne – 3 szt.

W ramach postępowania wymagane 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.
- Wbudowany redundantny zasilacz.
- Maksymalny pobór mocy: 50 W.
- Minimalny zakres temperatury pracy: 0-50°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

e) 4 porty 10 GE SFP+.

Zarządzanie

- Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
- Wbudowany 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.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Parametry wydajnościowe

- Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32 k 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.
- Wsparcie dla Private VLAN.
- Obsługa routingu statycznego.
- Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
- 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.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- Automatyczna detekcja i rekomendacje konfiguracji.
- Przesyłanie logów na zewnętrzny serwer syslog.
- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Obsługa białych i czarnych list adresów MAC.
- Wykrywanie aplikacji komunikujących się w sieci.

2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- 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 36 miesięcy**, 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.

Rozszerzone wsparcie serwisowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez **okres 36 miesięcy**.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien posiadać dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Oprogramowanie klasy SIEM

I. Przedmiot zamówienia:
   1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
   2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.

II. Wymagania techniczne dotyczące rozwiązania
   1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.
   2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na fizycznym serwerze będącym na wyposażeniu Zamawiającego, wirtualnej maszynie w środowisku Vmware lub wirtualnej maszynie w środowisku Hyper-V.
   3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
   4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną lub serwer fizyczny o następujących parametrach:
      - Procesor (CPU): 8 rdzeni,
      - Pamięć RAM: 16 GB,
      - Dysk twardy (HDD): 2 TB.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.

III. Wdrożenie systemu

1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego serwerze fizycznym lub maszynie wirtualnej.
4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspójniające zegary czasów w sieci Zamawiającego.
5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.
6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.
7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
   - 2 urządzenia klasy UTM ,
   - 3 przełączniki zarządzalne ,
   - serwery
   - 50 stacji roboczych
   - 1 aplikację centralnego zarządzania oprogramowaniem antywirusowym

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.
9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
14. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

Oprogramowanie klasy EDR

Oprogramowanie antywirusowe z EDR – na 45 stanowisk. Zakup przedłużenia (min.36 miesięcy) i rozszerzenia licencji oprogramowania antywirusowego posiadanego przez Zamawiającego wraz z wdrożeniem na miejscu połączonym z instruktażem.

Licencje muszą zostać dostarczone w podziale na dwa typy środowisk (Zamawiający nie dopuszcza licencjonowania urządzeń mobilnych/smartfonów):

- **Licencje na stacje robocze (komputery stacjonarne i laptopy):** w ilości **45 szt.**

  W celu zapewnienia bezwzględnej ciągłości działania oraz pełnej ochrony posiadanej infrastruktury, dostarczone oprogramowanie (agenci EDR) musi być w pełni kompatybilne, natywnie wspierane i stabilnie działać w środowisku systemów operacyjnych z rodziny Microsoft Windows 10 Professional oraz Microsoft Windows 11 Professional (wersje 64-bitowe) użytkowanych przez Zamawiającego.

- **Licencje na środowiska serwerowe:** w ilości **3 szt.** dedykowane i zoptymalizowane pod systemy operacyjne (w tym dla nowo wdrażanych maszyn wirtualnych).

  W celu zapewnienia ciągłości działania krytycznych usług urzędu oraz ochrony danych osobowych, dostarczone oprogramowanie (agenci EDR) musi być w pełni kompatybilne, stabilne oraz oficjalnie wspierane przez producenta EDR na systemach operacyjnych z rodziny Microsoft Windows Server (wersje 2016, 2019, 2022 oraz najnowszej 2025) w wersjach Standard oraz Datacenter

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Wykonawca w ramach zamówienia jest zobowiązany do instalacji, konfiguracji oraz pełnego uruchomienia agentów EDR na nowo dostarczonym serwerze fizycznym oraz na utworzonych w ramach licencji Microsoft na nowych maszynach wirtualnych.

Wszystkie zakupione licencje (zarówno stacyjne, jak i serwerowe) muszą być zarządzane centralnie z poziomu **jednej, wspólnej konsoli administracyjnej**

Oprogramowanie antywirusowe dla stacji roboczych i serwerów musi stanowić zintegrowany system ochrony nowej generacji klasy EPP/EDR, zarządzany z jednej, centralnej konsoli. System musi zapewniać ochronę w czasie rzeczywistym opartą na analizie behawioralnej (wykrywanie zagrożeń zero-day i bezplikowych) oraz oferować funkcje aktywnego reagowania na incydenty, w tym: automatyczną izolację sieciową zainfekowanej stacji, zdalne zabijanie złośliwych procesów oraz mechanizm automatycznego przywracania (rollback) plików zaszyfrowanych przez oprogramowanie typu ransomware. Narzędzie musi umożliwiać pełną analizę śledczą incydentu poprzez graficzną wizualizację drzewa procesów, w tym:

Administracja zdalna

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
    - 5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
    - 5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
    - 5.3. Buforowanie ruchu HTTPS.
6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
    - 7.1. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
        - 7.1.1. Google Authenticator,
        - 7.1.2. Microsoft Authenticator,
        - 7.1.3. Authy,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

7.1.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.

8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.

9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

9.1. 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:

9.1.1. adresy sieciowe IP,

9.1.2. aktywne zagrożenia,

9.1.3. stan funkcjonowania oraz ochrony,

9.1.4. wersja systemu operacyjnego,

9.1.5. podzespoły komputera.

10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:

10.1. wyrażenie CRON,

10.2. codziennie,

10.3. cotygodniowo,

10.4. co miesiąc,

10.5. co rok,

10.6. po wystąpieniu nowego zdarzenia,

10.7. po automatycznym umieszczeniu hosta w grupie dynamicznej.

11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim

11.1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania

12. Rozwiązanie musi mieć możliwość tagowania obiektów.

13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

13.1. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.

Ochrona stacji roboczych - Windows (posiadane przez Zamawiającego)

1. Rozwiązanie musi wspierać systemy operacyjne posiadane przez zamawiającego
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

3.3. robak,
3.4. adware,
3.5. spyware,
3.6. dialer,
3.7. phishing,
3.8. backdoor.

4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
   7.1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
   7.2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
   7.3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    10.1. całego dysku,
    10.2. wybranych katalogów,
    10.3. pojedynczych plików,
    10.4. plików spakowanych oraz skompresowanych,
    10.5. dysków sieciowych,
    10.6. dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    11.1. wybranych plików,
    11.2. wybranych procesów,
    11.3. wybranych lokalizacji,
    11.4. wybranych rozszerzeń,
    11.5. nazwy wykrycia,
    11.6. sumy kontrolnej (SHA1).
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
    13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. 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).
15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    17.1. typ urządzenia:
        17.1.1. pamięci masowe,
        17.1.2. optyczne pamięci masowe,
        17.1.3. pamięci masowe Firewire,
        17.1.4. urządzenia do tworzenia obrazów,
        17.1.5. drukarki USB,
        17.1.6. urządzenia Bluetooth,
        17.1.7. czytniki kart inteligentnych,
        17.1.8. modemy,
        17.1.9. porty LPT/COM, 17.1.10. urządzenia przenośne.
    17.2. parametry urządzenia:
        17.2.1. numer seryjny, 17.2.2. producent,
        17.2.3. model.
    17.3. typ dostępu:
        17.3.1. brak możliwości zapisu,
        17.3.2. pełen dostęp,
        17.3.3. ostrzeżenie użytkownika, 17.3.4. brak dostępu.
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

18.4. 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,

18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

19.1. 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.

19.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

19.3. Raport musi posiadać co najmniej:

19.3.1. Listę zainstalowanych aplikacji,

19.3.2. Listę usług systemowych,

19.3.3. Informacje o systemie operacyjnym i sprzęcie,

19.3.4. Listę aktywnych procesów i połączeń sieciowych,

19.3.5. Harmonogram systemu operacyjnego,

19.3.6. Szczegóły pliku hosts,

19.3.7. Informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu

20.1. antywirus,

20.2. zapora osobista

20.3. sandbox,

20.4. antyspyware,

20.5. metody heurystyczne.

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

22.1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.

22.2. Ochrona musi być realizowana w oparciu o co najmniej:

22.1.1. globalna czarna lista RBL,

22.1.2. czarna lista użytkownika,

22.1.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.

23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:

23.1.1. Skanowanie portów TCP oraz UDP,

23.1.2. Wykrywanie duplikacji adresu IP,

23.1.3. Atak zatruwania ARP,

23.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.

23.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:

23.2.1. RDP,

23.2.2. SMB,

23.2.3. My SQL,

23.2.4. MS SQL.

23.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

24.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

24.2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

24.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

24.2.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

24.2.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

24.2.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

24.2.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.

25.1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

25.2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

25.3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.

26.1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.

26.2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: Treść komunikatu i Obraz.

Ochrona serwera – Windows Server (lub równoważny)

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   1.1. Microsoft Windows Server 2012 R2,
   1.2. Microsoft Windows Server 2016,
   1.3. Microsoft Windows Server 2019,
   1.4. Microsoft Windows Server 2022,
   1.5. Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   3.1. wirus,
   3.2. trojan,
   3.3. robak,
   3.4. adware,
   3.5. spyware,
   3.6. dialer,
   3.7. phishing,
   3.8. 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.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
   8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   9.1. całego dysku,
   9.2. wybranych katalogów,
   9.3. pojedynczych plików,
   9.4. plików spakowanych oraz skompresowanych,
   9.5. dysków sieciowych,
   9.6. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   10.1. wybranych plików,
   10.2. wybranych procesów,
   10.3. wybranych lokalizacji,
   10.4. wybranych rozszerzeń,
   10.5. nazwy wykrycia,
   10.6. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
   12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
   12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
   12.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
   12.4. 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,
   12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    13.1. 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.
    13.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
    13.3. Raport musi posiadać co najmniej:
        13.3.1. Listę zainstalowanych aplikacji,
        13.3.2. Listę usług systemowych,
        13.3.3. informacje o systemie operacyjnym i sprzęcie,
        13.3.4. Listę aktywnych procesów i połączeń sieciowych,
        13.3.5. harmonogram systemu operacyjnego,
        13.3.6. Szczegóły pliku hosts,
        13.3.7. Informacje o sterowników.
14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
    14.1. antywirus,
    14.2. zapora osobista
    14.3. sandbox,
    14.4. antyspyware,
    14.5. metody heurystyczne.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    17.1. typ urządzenia:
        17.1.1. pamięci masowe,
        17.1.2. optyczne pamięci masowe,
        17.1.3. pamięci masowe Firewire,
        17.1.4. urządzenia do tworzenia obrazów,
        17.1.5. drukarki USB,
        17.1.6. urządzenia Bluetooth,
        17.1.7. czytniki kart inteligentnych,
        17.1.8. modemy,
        17.1.9. porty LPT/COM, 17.1.10. urządzenia przenośne.
    17.2. parametry urządzenia:

17.2.1. numer seryjny, 17.2.2. producent,
17.2.3. model.

17.3. typ dostępu:
17.3.1. brak możliwości zapisu,
17.3.2. pełen dostęp,
17.3.3. ostrzeżenie użytkownika, 17.3.4. brak dostępu.

18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
18.1. MS SQL,
18.2. Active Directory,
18.3. IIS,
18.4. Sysvol,
18.5. DNS,
18.6. DHCP,
18.7. Hyper-V,
18.8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
19.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
19.1.1. Skanowanie portów TCP oraz UDP,
19.1.2. Wykrywanie duplikacji adresu IP,
19.1.3. Atak zatruwania ARP,
19.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.
19.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
19.2.1. RDP,
19.2.2. SMB,
19.2.3. My SQL,
19.2.4. MS SQL.
19.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
21.1. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
21.1.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

21.1.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
21.1.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
21.1.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
21.1.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Zwiększenie funkcjonalności o moduł EDR

1. Moduł EDR / XDR pochodzący od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
   - 3.1. tworzenie procesów,
   - 3.2. uruchamianie, zatrzymanie i modyfikacja usług,
   - 3.3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,
   - 3.4. usuwanie oraz zmiana nazw plików,
   - 3.5. tworzenie i usuwanie kluczy rejestru systemowego,
   - 3.6. ładowanie bibliotek DLL,
   - 3.7. zalogowanie użytkowników,
   - 3.8. elementy sieciowe, w tym co najmniej
     - 3.8.1. pobranie plików wykonywalnych,
     - 3.8.2. zestawienie połączeń TCP/IP,
     - 3.8.3. zapytania HTTP,
     - 3.8.4. zapytania DNS.
4. Rozwiązanie musi posiadać minimum 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.
   - 4.1. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
     - 4.1.1. blokowanie pliku wykonywalnego,
     - 4.1.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,
     - 4.1.3. blokowanie podejrzanej biblioteki DLL,
     - 4.1.4. zakończenie procesu,
     - 4.1.5. skanowanie komputera w poszukiwaniu zagrożeń,
     - 4.1.6. wyłączenie komputera,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

4.1.7. izolacja sieciowa hosta,
4.1.8. wylogowanie użytkownika.

4.2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5.1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.

5.2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:

5.2.1. proces,
5.2.2. proces nadrzędny (proces rodzica),
5.2.3. nazwę procesu,
5.2.4. ścieżkę procesu,
5.2.5. wiersz polecenia,
5.2.6. wydawcę,
5.2.7. typ podpisu,
5.2.8. SHA-1,
5.2.9. SHA-2,
5.2.10. użytkownika.

5.3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.

6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.

6.1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.

6.2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):

6.2.1. SHA-1,
6.2.2. SHA-256.

7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:

7.1. hash pliku SHA-1,
7.2. hash pliku SHA-256,
7.3. hash pliku MD5,
7.4. typ sygnatury podpisu cyfrowego,
7.5. wydawcę certyfikatu,
7.6. wersję pliku,
7.7. oryginalną nazwę pliku,
7.8. rozmiar pliku,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

7.9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,
7.10. pierwsze uruchomienie pliku w środowisku,
7.11. ostatnie uruchomienie pliku w środowisku,

8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
8.1. oznaczania ich jako bezpieczne lub niebezpieczne,
8.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
8.3. zablokowania wykonywania i wykorzystania pliku,
8.4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.

9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
9.1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
9.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
9.3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
9.4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
10.1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.

11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.

12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików

Cechy techniczne systemu EDR

- **Wspólna telemetria:** System musi korelować zdarzenia zachodzące na stacjach roboczych urzędników ze zdarzeniami rejestrowanymi na serwerze, umożliwiając wykrywanie tzw. *lateral movement* (prób bocznego przemieszczania się hakera w sieci urzędu ze stacji na serwer).
- **Ochrona procesów serwerowych:** Moduł EDR przeznaczony na serwer musi posiadać funkcję aktywnej ochrony pamięci RAM oraz mechanizm blokowania prób wyłączenia usług antywirusowych (tzw. *Anti-tampering*)

Zakres wdrożenia na miejscu:

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

1. Aktywacja serwera ESET Inspect.
2. Wdrożenie konektorów ESET Inspect Connector.
3. Stworzenie maksymalnie 3 wyjątków dla rozwiązania ESET Inspect.

W celu wdrożenia wykonawca doinstaluje niezbędne komponenty systemu

Ad. 2g Audyt bezpieczeństwa

Przedmiotem zamówienia jest przeprowadzenie audytu oraz opracowanie kompleksowej polityki bezpieczeństwa w zakresie cyberbezpieczeństwa w Urzędzie Gminy Niegowa. Celem audytu jest ocena obecnego stanu zabezpieczeń informatycznych Urzędu, identyfikacja zagrożeń oraz wskazanie obszarów wymagających poprawy. Na podstawie wyników audytu wykonawca opracuje i dostarczy dokumentację polityki bezpieczeństwa, która będzie zgodna z obowiązującymi przepisami prawa oraz standardami najlepszych praktyk w zakresie ochrony danych i systemów informacyjnych.
Zakres zamówienia:

1. **Audyt bezpieczeństwa:**

Wykonawca przeprowadzi audyt bezpieczeństwa systemów teleinformatycznych Urzędu Gminy Niegowa w celu oceny obecnego stanu zabezpieczeń, identyfikacji podatności i zagrożeń oraz wskazania obszarów wymagających poprawy. Na podstawie wyników audytu Wykonawca opracuje i dostarczy kompleksową dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym Politykę Bezpieczeństwa Informacji, w pełni dostosowaną do struktury i specyfiki Urzędu. Efektem końcowym audytu musi być **sporządzenie Raportu z audytu** oraz obowiązkowe **wypełnienie przez audytora Ankiety Dojrzałości Cyberbezpieczeństwa**, stanowiącej załącznik do wniosku rozliczającego projekt „Cyberbezpieczny Samorząd”

Zakres obejmuje w szczególności:

- Przeprowadzenie szczegółowej analizy infrastruktury IT Urzędu Gminy Niegowa, w tym systemów informacyjnych, sieci komputerowych, urządzeń końcowych, aplikacji i baz danych.
- Ocena ryzyka związanego z cyberzagrożeniami, w tym analiza podatności systemów na ataki zewnętrzne i wewnętrzne.
- Weryfikacja przestrzegania procedur bezpieczeństwa, polityk dostępu oraz ochrony danych osobowych.
- Identyfikacja luk w zabezpieczeniach oraz rekomendacja działań naprawczych.
- Audyt musi zostać przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Audyt musi zostać przeprowadzony w zakresie spełniającym wymagania określone w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad

2. **Opracowanie polityki bezpieczeństwa:**

- Opracowanie dokumentu Polityki Bezpieczeństwa IT, który będzie stanowił zbiór zasad, procedur i wymagań dotyczących ochrony zasobów informacyjnych Urzędu Gminy Niegowa.
- Określenie odpowiedzialności za zarządzanie bezpieczeństwem informacji w Urzędzie Gminy Niegowa.
- Zdefiniowanie procedur zarządzania incydentami bezpieczeństwa oraz planu reagowania na cyberzagrożenia.
- Zapewnienie zgodności z obowiązującymi przepisami prawa, w tym ustawą o ochronie danych osobowych, RODO, a także normami ISO/IEC 27001 w zakresie zarządzania bezpieczeństwem informacji.

Opracowana dokumentacja oraz przeprowadzony audyt muszą być zgodne z:Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773),Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Międzynarodowymi normami serii ISO/IEC 27001 oraz ISO/IEC 22301 (w zakresie ciągłości działania)

Wymagania dotyczące wykonawcy:

Wykonawca zobowiązany jest skierować do realizacji tego zadania co najmniej jedną (1) osobę, która posiada uprawnienia i kwalifikacje do przeprowadzania audytów weryfikujących spełnienie wymogów bezpieczeństwa, potwierdzone:

- Legitymowaniem się uprawnieniami audytora określonymi w § 21 ust. 2 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności... (np. certyfikat CISA, CISM, CISSP, CRISC, ISO/IEC 27001 Lead Auditor wydany przez jednostkę akredytowaną lub odpowiedni dyplom studiów podyplomowych),
- lub legitymowaniem się certyfikatem ujętym w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (wydanym na podstawie ustawy o krajowym systemie cyberbezpieczeństwa)

Audytor winien posiadać wiedzę z zakresu regulacji prawnych związanych z ochroną danych osobowych, w tym RODO.
Audytor musi posiadać doświadczenie polegające na należytym przeprowadzeniu w okresie ostatnich 5 lat przed upływem terminu składania ofert co najmniej dwóch (2) audytów bezpieczeństwa informacji (zgodności z KRI lub SZBI) w jednostkach sektora finansów publicznych, zakończonych sporządzeniem raportu z audytu.

Zasilacz awaryjny UPS

Opis zasilacza UPS o mocy 15kVA:

PARAMETR	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
Typ urządzenia	Zasilacz awaryjny

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Topologia	Online/podwójna konwersja
Obudowa	Tower
Wartość znamionowa (VA)	Min. 15 000 VA
Moc	Min. 12 000 W
Zakres napięcia wyjściowego	220/230/240 V +/- 2%
Kształt fali na wyjściu	Sinusoida
Wyjściowy współczynnik mocy	0,8
Napięcie znamionowe wejściowe	400V/230V
Częstotliwość znamionowa wejściowa	50/60 Hz
Współczynnik mocy wejściowej	> 0,99
Zakres napięcia wejściowego	176-276 V (110-276 V przy obniżeniu)
Zakres częstotliwości wejściowych	45-66Hz
Rodzaj akumulatora	Szczelne, kwasowo-ołowiowe, żywotność min.10 lat
Liczba akumulatorów	40
Zarządzanie akumulatorem	• Automatyczny test baterii • Ochrona przed głębokim rozładowaniem
Parametry znamionowe akumulatora	12 V / 7 Ah
Łączność	• Port USB (komptybilny z HID) • Port seryjny (RS232) • Mini-terminal zacisków do zdalnego wyłączania • Gniazdo komunikacji
Interfejs użytkownika	Wyświetlacz LCD
Gniazda rozszerzeń	Jedno gniazdo na opcjonalną kartę komunikacyjną
Poziom hałasu	Mniej niż 55 dB w odległości 1 m
Zakres temperatury pracy	od 0° do 40°C
Wilgotność względna	0-95%, bez kondensacji
Sprawność	93%
Faza (wyjście)	1
Wewnętrzne obejście	Tak
Wymiary maks. (gł. x wys. x sz.)	71cm x 82 cm x 36 cm
Zgodność/zgodności	• CE • TUV
Certyfikat(y)	• IEC/EN 62040-1 • IEC/EN 62040-2

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

	• CE • EAC
Zawartość zestawu	• UPS • Kabel USB • Kabel szeregowy • Podręcznik użytkownika
Gwarancja	12 miesięcy gwarancji producenta door to door na elektronikę i na akumulatory

Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego.
- Wykonawca zobowiązany jest wykonać podłączenie do istniejącej instalacji elektrycznej przygotowanej przez Zamawiającego zgodnie z wytycznymi producenta UPS.
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).

Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Urządzenie NAS

Procesor	Czterordzeniowy procesor AMD Ryzen V1780B 3,35 GHz (częstotliwość podstawowa) lub równoważny
Obudowa	Rack 1U o wymiarach max. 45 × 482 × 556 mm; szyny teleskopowe do instalacji w szafie RACK
Pamięć RAM	Pamięć 8 GB DDR4 ECC UDIMM (z możliwością rozszerzenia do 32 GB)
Ilość obsługiwanych dysków	12 dysków 2,5" SATA SSD
Ilość zainstalowanych dysków	4 dyski SSD klasy Enterprise w formacie 2,5” znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 3,84TB; Możliwość aktualizacji oprogramowania dysku z poziomu NAS.
Interfejsy sieciowe	2 porty 1GbE RJ-45 2 porty 10 GbE RJ-45
Porty	2 porty USB 3.2 1. generacji 1x PCIe 4-liniowe gniazdo x8 generacji 3
Wskaźniki LED	Zasilanie, alert, status, LAN, HDD1-12
Obsługa RAID	F1, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Licencja na Kamery IP	W zestawie dwie licencje na jedną kamerę z możliwością rozszerzenia do 100.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP i VPN (PPTP, OpenVPN™, L2TP)
Usługi	Wsparcie dla High Availability Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antyvirus Klient VPN Usługa DDNS Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware
Obsługa migawek	• Maksymalna liczba migawek na foldery współdzielone: 256 • Maksymalna liczba migawek systemu: 4096
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
Język GUI	Polski
Gwarancja i serwis	5 lat gwarancji door-to-door producenta lub autoryzowanego partnera producenta na urządzenie oraz dyski

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską

Certyfikaty	CE
System plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT
Liczba wolumenów	Do 256
Liczba iSCSI Targetów	Do 64
Liczba iSCSI LUN	Do 128
Liczba grup	512
Liczba udziałów	512
Chłodzenie	FAN x 4 40 x 40 mm

Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego.
- Na zaoferowanym urządzeniu musi zostać przeprowadzona aktualizacja oprogramowania systemowego. Urządzenie zostanie skonfigurowane zgodnie z najlepszymi praktykami.
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonego systemu obejmujące przynajmniej omówienie konfiguracji i funkcji.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Centrum Projektów Polska Cyfrowa | Dofinansowane przez Unię Europejską