Załącznik nr 6
Do zapytania ofertowego
(załącznik nr 2 do umowy)

OPZ – Opis przedmiotu zamówienia

Zamawiający:
GMINA Korczew,

ul. Księdza Stanisława Brzóski 20a

08-108 Korczew

NIP 8212392351,

Podniesienie poziomu bezpieczeństwa cyfrowego danych przetwarzanych w Urzędzie Gminy Korczew przez wdrożenie SZBI, podniesienie świadomości oraz zakup sprzętu zwiększającego bezpieczeństwo" w ramach realizacji umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1271/ FERC.02.02-CS.01-001/23/2024

Wstęp

W ramach zadania Wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia.

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich elementów opisanych w tym dokumencie):

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,

- Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.

- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem);

- Zamawiający wymaga, by dostarczone licencje na oprogramowanie i systemy operacyjne były nowe i nie były nigdy wcześniej aktywowane czy używane na innych urządzeniach;

- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;

- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów sprzętu.

- Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku bankructwa Wykonawcy niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);

- Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;

- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach:

230 V ±10%, 50Hz;

- W cenę musi być wliczony koszt dostawy – transportu oraz w przypadku sprzętu montażu w szafie krosowej lub innym wskazanym miejscu;

- Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego w dni powszednie w godzinach 8-15;

- Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania;

- Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne.

Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:

a) połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),

b) łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,

c) zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,

d) wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem.

W szczególności wymagany zakres obejmuje:

CZĘŚĆ I ZAMÓWIENIA - Dostawa UTM, tokenów, AP, przełącznika

1.1. **Wsparcie dla posiadanego UTM FortiGate 40F**

Producent Fortinet - FortiGate typ wsparcia – nazwa Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów do 30 czerwca 2026 dla urządzenia Fortigate 40F o numerze seryjnym FGT40FTK22099N26. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do 30 czerwca 2026.

Wsparcie

1. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje:
   - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 650 tys. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 950 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall uwzględnia adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować 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
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania dostarcza oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

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

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System ma możliwość wstrzymania dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres wsparcia produktu.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. System zapewnia możliwość logowania do serwera SYSLOG.
5. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Rozszerzone wsparcie

Do zamawianego produktu Wykonawca zapewni usługi wsparcia technicznego świadczona w języku polskim w zakresie co najmniej:

a) pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu;

b) zdalna rekonfiguracja produktu (połączenia szyfrowane) zgodnie z wymaganiami użytkownika max. 15 godzina zegarowych rozliczanych do 15 minut w terminie wsparcia produktu;

1.2. **Token do UTM - 5 sztuk**

Producent..... Model.....
Rok produkcji.....

Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych.

1. W ramach postępowania powinny zostać dostarczone 5 tokenów sprzętowych współpracujące bezpośrednio z posiadanym UTM 40F, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site.

1.3. **<u>Wewnętrzny bezprzewodowy punkt dostępowy – 1 sztuki</u>**

Punkt dostępowy tuneluje cały ruch kliencki do kontrolera bezprzewodowego, działającego w obrębie platformy UTM, dzięki czemu Administrator może z poziomu jednej konsoli zarządzać bezpieczeństwem całego ruchu w sieci, również bezprzewodowej. Otrzymuje korzyści w postaci lepszej przejrzystości sieci, spójnych metod egzekwowania reguł bezpieczeństwa oraz uproszczenia środowiska sieciowego.

Producent..... Model..... Rok produkcji.....	
Nazwa parametru, elementu lub cechy	**Wymagane parametry techniczne**
Min. parametry fizyczne	Technologia RF: 2x2 802.11ac Wave 2 Radio 1: 2.4 GHz b/g/n (2x2:2stream) 20/40 MHz (256 QAM) Radio 2: 5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM) Anteny wewnętrzne: 4 + 1 BLE Porty: 1 x port 10/100/1000 RJ45, BT/BLE. Maksymalna szybkość transmisji danych: Radio 1: do 400 Mbps, Radio 2: do 867 Mbps

	Pasma częstotliwości (GHz): 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850 Zestaw do montażu sufitowego/ściennego: TAK Zasilanie: Iniektor 802.3af PoE GPI-115 lub zasilacz
Zarządzanie z konsoli UTM	Punkt dostępowy tuneluje cały ruch kliencki do kontrolera bezprzewodowego, działającego w obrębie platformy UTM,
parametry	Punkty dostępowe AP wykorzystują technologię 802.11n w celu zagwarantowania wysokiej przepustowości sieci bezprzewodowej, umożliwiają uruchomienie kilku SSID na pojedynczym module radiowym oraz opcję monitoringu otoczenia i wykrywania obcych punktów dostępowych. Pracują w połączeniu z bogatymi w funkcje kontrolerami UTM w celu dostarczenia umocnionej przestrzeni bezprzewodowej zapewniającej kompletną ochronę ruchu.
	Technologia 802.11n zapewnia przepustowości rzędu 300Mbps na moduł radiowy oraz zasięg dwukrotnie większy niż dla standardów 802.11a/b/g.

	Silne metody uwierzytelnienia wykorzystujące WPA2 enterprise.
	Obsługa Power Over Ethernet (POE) eliminuje konieczność wykorzystania zewnętrznego zasilacza.
	Możliwość priorytetyzacji ruchu bezprzewodowego dla krytycznych aplikacji.
	Polityki bazujące na tożsamości użytkowników w połączeniu z wykrywaniem i raportowaniem obcych punktów dostępowych, granularna kontrola punków końcowych, szablony raportów zgodnych z wymaganiami audytowymi zapewniają zgodność z wymaganiami prawnymi w kontekście dostępu i ochrony danych.
	Elastyczne opcje wdrożenia rozwiązania w połączeniu z konsolą zarządzania na UTM i brakiem dodatkowych opłat licencyjnych.
	Zwiększona przejrzystość działań i kontrola użytkowników i aplikacji z urządzeniem UTM zapewniającym kompletną ochronę przesyłanych treści oraz identyfikację i powstrzymanie zagrożeń.

Gwarancja i wsparcie	**Do 30 czerwca 2026**.

Dostawa i montaż: Dostawa do Zamawiającego oraz wstępna konfiguracją ustalona z Zamawiającym – max. 1 godzina zegarowa.

1.4. **<u>Dostawę przełączników sieci LAN – 1 sztuki – o parametrach nie gorszych niż:</u>**

Producent..... Model..... Rok produkcji.....	
Nazwa parametru, elementu lub cechy	**Wymagane parametry techniczne**
Parametry fizyczne	- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. - Zasilanie AC 230V.
Interfejsy sieciowe	- 48 porty GE RJ-45.4 gniazdami SFP+ 10 Gbps SR. **z zainstalowaną wkładką – 4 sztuki**

Zarządzanie	- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS), **oraz z poziomu UTM dostarczanego w ramach niniejszego postępowania.** - Wsparcie dla SNMP w wersjach 1-3 - Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. - Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. - Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. - Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). - Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. - Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. - Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe	- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. - Tablica adresów MAC o pojemności co najmniej 32k wpisów. - Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. - Obsługa Jumbo Frames. - Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). - Agregacja portów zgodna ze standardem 802.3ad. - Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. - Obsługa routingu statycznego. - Port-mirroring. - Uwierzytelnianie 802.1x na poziomie portu. - Uwierzytelnianie 802.1x w oparciu o adres MAC. - W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). - W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. - W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

	- Obsługa protokołu sFlow.
Gwarancja	- Minimum do **30 czerwca 2026** - System musi być objęty serwisem gwarancyjnym producenta, 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.

Dostawa i montaż:

Dostawa wraz z instalacją w szafie krosowej u Zamawiającego oraz wstępna konfiguracją ustalona z Zamawiającym – max. 3 godzin zegarowych na miejscu u Zamawiającego.

CZĘŚĆ II ZAMÓWIENIA- Dostawa serwera do cyberbezpieczeństwa, oprogramowania systemowego, dysków do NAS, UPS

2.1 <u>Serwer dla usług cyberbezpieczeństwa – 1 sztuka</u>

Producent..... Model.....

Rok produkcji.....

Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;

Na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta zgodnie w informację przy danym sprzęcie; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego (24 godziny);

Zakres dostawy - serwer

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania ramienia porządkującego kable;
- Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;
- Zainstalowane zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Możliwość zainstalowania 2 dysków SSD M.2 PCIe
- Zainstalowane 5 szt. dysków 2,5” SSD SATA o pojemności min. 960GB typu Read-Intensive

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express generacji 5 w tym:
    - 4 fizyczne złącza o prędkości x16;
    - 2 fizyczne złącza o prędkości x8;
    - Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
    - Opcjonalnie możliwość uzyskania min. 8 aktywnych interfejsów PCI-e w konfiguracji dwuprocesorowej;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM DDR5;
- Wsparcie dla technologii:
    - Memory Scrubbing;
    - SDDC;
    - ECC;
    - Memory Mirroring;
    - ADDDC;

Procesory

- Zainstalowane dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64; osiągające w teście SPEC CPU2017 Integer Rate Result wynik SPECrate2017_int_base min. 150 pkt. (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html [spec.org]

Pamięć RAM

- 128 GB pamięci RAM w kościach 64GB;
- DDR5 Registered 4800MT/s;

Kontrolery LAN

- 2x10G SFP+ wraz z dołączonymi wkładkami wielomodowymi
- Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:
  - 1x 1Gbit Base-T;
  - 4x1 Gbit Base-T;

Kontrolery I/O

- Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60
- Kontroler musi być wyposażony w mechanizm umożliwiający podtrzymanie pamięci cache w razie utraty zasilania

Porty

- Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- 2 porty USB 3.0 dostępne z tyłu serwera;
- 1 port USB wewnętrzny
- 2 porty USB 3.0 na panelu przednim;
- Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hot-plug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hot-plug.
- Kable zasilające typu C13-C14 o długości min. 2m

Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
    - informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
        - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
        - procesory CPU;
        - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
        - status karty zarządzającej serwera;
        - wentylatory;
        - bateria podtrzymująca ustawienia BIOS płyty głównej;
        - zasilacze;
        - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
    - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
    - Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
    - Dostęp poprzez przeglądarkę Web, SSH;
    - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
    - Zarządzanie alarmami (zdarzenia poprzez SNMP);
    - Możliwość przejęcia konsoli tekstowej;
    - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
    - Obsługa serwerów proxy (autentykacja);
    - Obsługa VLAN;
    - Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
    - Wsparcie dla protokołu SSDP;
    - Obsługa protokołów TLS 1.2, SSL v3;
    - Obsługa protokołu LDAP;
    - Synchronizacja czasu poprzez protokół NTP;
    - Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);

- Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2022, 2019;
- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2022.

Gwarancja

- 4 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis – **w ofercie należy podać koszt serwera z gwarancją do 30 czerwca 2026 oraz koszt gwarancji na pozostały okres jako odrębną pozycję kosztowa.**
- Uszkodzone dyski nie podlegają zwrotowi organizacji serwisującej
- Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;

- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
- Zgodność z normami: CB, RoHS, WEEE oraz CE.

Dostawa i montaż:

- Dostawa wraz z instalacją u Zamawiającego w szafie krosowej, instalacja systemu operacyjnego konfiguracja replikacji danych z posiadanym przez Zamawiającego serwerem – max. 16 godzin zegarowych na miejscu u Zamawiającego.

2.2 Licencja dla serwera - Serwerowy system operacyjny (SSO)

Serwerowe systemy operacyjne dla serwerów		
Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane minimalne parametry techniczne**
	1	**2**
1.	**Oprogramowanie**	Zamawiający wymaga dostarczenia licencji na najnowszą dostępną wersję serwerowego systemu operacyjnego w chwili podpisania umowy (w polskiej wersji językowej), wyposażonego w odpowiednią ilość licencji obejmujących wszystkie fizyczne rdzenie procesora w serwerze. **System operacyjny musi spełniać wymogi punktu 2 (Funkcjonalności i kryteria) oraz być dostarczony w odpowiedniej ilości licencji aby spełnić wymagania:** • Umożliwiać uruchomienie **4 maszyn wirtualnych z tym systemem operacyjnym** na dostarczonym serwerze. • Umożliwiać uruchomienie **nieograniczonej liczby maszyn**

		wirtualnych z innymi systemami operacyjnymi (np. Linux). Zamawiający wymaga dokupienie **dodatkowej licencji do posiadanego serwera** celem rozszerzać możliwości posiadanego przez Zamawiającego systemu serwerowego z 2019 (MSW2019STD) r. o **dwie dodatkowe maszyny wirtualne** na obecnym sprzęcie serwerowym (dwa procesory 8-rdzeniowe). **Zamawiający wymaga uruchomienia replikacji danych co 30 sekund między kupowanym i posiadanym serwerem w ramach funkcjonalności posiadanej przez serwerowy system operacyjny.** **Wykonawca łącznie ma dostarczyć 3 sztuki serwerowego systemu operacyjnego dwa na nowo kupowany serwer oraz jedną na posiadany serwer w najnowszej wersji. System musi umożliwiać bez stosowania emulatorów uruchomienia używanych aplikacji używanych w UG.** Dostarczone licencje muszą upoważniać do użytkowania dostarczonego oprogramowania na czas nieokreślony.
	Zamawiający wymaga spełnienia przez serwerowy system operacyjny wymagań w zakresie funkcjonalności określonych poniżej:	
2.	**Funkcjonalności i kryteria**	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności

		stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,

		o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze,

		IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez

		oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

2.3 <u>Dysk twardy do macierzy dyskowej NAS – 1 sztuki</u>

Dyski twarde do macierzy dyskowej Synology RS822+ **dyski muszą być na liście kompatybilności NAS.**	**……** **Typ / model / producent** **Minimalne wymagania**
Dysk twardy 16TB	**przeznaczony dla systemów NAS pracującym w systemie ciągłym**

Pojemność	min. 16 TB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	SATA III (6 Gb/s)
Pamięć cache	min. 256 MB
Prędkość obrotowa	7200 obr./ min.
MTBF	**1000000 h**
Gwarancja	**Standardowa gwarancja producenta min. 24 miesiące.**

CZĘŚĆ III ZAMÓWIENIA - Dostawa oprogramowania do monitorowania sieci LAN, backup w chmurze, EDR/XDR oraz centralnego logowania logów

3.1 <u>Oprogramowanie do monitorowania sieci LAN, zarządzania użytkownikami, zarządzania zasobami IT</u>

Producent..... Nazwa.....

wersja .....

Licencja do monitorowania sieci LAN, zarządzania użytkownikami, zarządzania zasobami IT i kontroli dostępu do danych dla pracowników Urzędu ma obejmować 24 stacji roboczych **do 30 czerwca 2026**.
Obecnie urząd posiada moduły Axence: NETWORK, INVENTORY, USER, a wymagane jest dodatkowo rozszerzenie licencji o moduł DATAGUARD (32 stacji do 30 czerwca 2026).
W ramach licencji producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne **do 30 czerwca 2026**. Oprogramowanie ma zawierać centralną konsolę do zarządzania instalowaną lokalnie. Oprogramowanie ma zawierać funkcje takie jak:

- skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
- interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
- jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
- serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
- liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
- działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
- liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
- kompilator plików MIB
- obsługa pułapek SNMP
- routery i switche: mapowanie portów
- obsługa komunikatów syslog
- alarmy zdarzenie - akcja
- powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)
- raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)
- tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów)
- komentarze, zrzuty ekranowe i załączniki w zgłoszeniach
- konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia
- automatyzacje bazujące na założeniu: warunek-> akcja
- przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”)
- dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę

- dwa tryby widoku - jasny i ciemny
- planowanie zastępstw w przydzielaniu zgłoszeń
- rozbudowany system raportów
- powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym
- baza zgłoszeń z rozbudowaną wyszukiwarką
- baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube
- przejrzysty i intuicyjny interfejs webowy
- wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych
- komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu
- zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury
- dwukierunkowa wymiana plików
- zarządzanie procesami Windows z poziomu okna informacji o urządzeniu
- zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)
- procesowanie zgłoszeń z wiadomości e-mail
- integracja bazy użytkowników z Active Directory
- zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
- audyt inwentaryzacji sprzętu i oprogramowania
- wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
- zdalny dostęp do managera plików z możliwością usuwania plików użytkownika
- informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej
- szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
- zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI
- alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
- lista kluczy oprogramowania Microsoft
- aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR
- możliwość archiwizacji i porównywania audytów
- monitorowanie harmonogramu zadań Windows
- redukcja kosztów wydruku
- blokowanie stron WWW
- blokowanie uruchamianych aplikacji
- monitorowanie wiadomości e-mail (nagłówki) - antyphishing
- szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)
- użytkowane aplikacje (aktywnie i nieaktywnie)
- odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
- audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
- użycie łącza: generowany przez użytkowników ruch sieciowy
- statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
- zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)
- blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE

- zarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników),
- automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa,
- monitorowanie operacji na plikach z zasobów sieciowych udostępnianych przez urządzenia nieobsługiwane przez Agenta np. macierze Synology, Qnap, itp.,
- zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych,
- integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych,
- integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów,
- możliwość zdalnego szyfrowania dysków za pomocą funkcji BitLocker,
- informacje o urządzeniach podłączonych do danego komputera,
- lista wszystkich urządzeń podłączonych do komputerów w sieci,
- audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych,
- zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników,
- centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory,
- integracja bazy użytkowników i grup z Active Directory,
- alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym

3.2 Backup w chmurze

Producent..... Nazwa..... wersja .....

W ramach postępowania powinna zostać dostarczona usługa upoważniająca do korzystania z backupu w chmurze posiadanych kopii lokalnych na urządzeniu NAS Synology RS822+.
Chmurowanie ma zapewniać rozmiar pamięci masowej w wielkości 5TB do 30 czerwca 2026.
Usługa musi zapewniać :

- Kopie zapasowe co godzinę,
- Dostosowywanie strategii przechowywania (wszystkie wersje kopii zapasowych są wliczane do limitu pamięci masowej, ale deduplikacja eliminuje powielone bloki danych w różnych wersjach kopii zapasowych),

- Usuwanie duplikatów danych,
- Udostępnianie i synchronizacja plików w wielu lokalizacjach,
- Lokalna pamięć podręczna dla często używanych danych,
- Przypinanie plików i folderów,
- **Dane na serwerach są chronione szyfrowaniem AES-256**

3.3 EDR/XDR

Producent..... Nazwa..... wersja .....

Obecnie urząd posiada **24 stanowiska oprogramowania ochrony punktów końcowych** działającego lokalnie (on-premise) ESET Protect Entry on-prem.

Nowa licencja na **oprogramowanie typu XDR (Extended Detection & Response)** ma obejmować 24 stanowisk do 30 czerwca 2026 r. od dnia dostawy. W ramach licencji producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne przez ten okres. Oprogramowanie ma zawierać centralną konsolę do zarządzania, instalowaną lokalnie.

Oprogramowanie musi zapewniać następujące funkcje ochrony:

1. **Stacje robocze – ochrona antywirusowa**:
    - Ochrona systemów operacyjnych takich jak **Windows, macOS i Linux** przed zagrożeniami wirusowymi.
2. **Stacje robocze – ochrona bezpieczeństwa**:

- Zabezpieczenie stacji roboczych na różnych platformach systemowych (Windows, macOS) przed złośliwym oprogramowaniem oraz atakami sieciowymi.

3. **Serwery plików**:

   - Ochrona serwerów plików, zapewniająca bezpieczeństwo przed zagrożeniami typu malware.

4. **Urządzenia mobilne z systemem Android**:

   - Zabezpieczenie urządzeń mobilnych przed zagrożeniami, w tym ochronę aplikacji i danych.

5. **Izolacja w chmurze (sandboxing)**:

   - Analiza podejrzanych plików w bezpiecznym, odizolowanym środowisku w chmurze, co zapewnia zaawansowaną ochronę przed nieznanymi zagrożeniami.

6. **Rozszerzona detekcja i odpowiedź (XDR)**:

   - System do zaawansowanej analizy i monitorowania incydentów bezpieczeństwa na urządzeniach końcowych, umożliwiający szybką reakcję na zagrożenia.

7. **Konsola zarządzająca**:

   - Centralne narzędzie zarządzania, pozwalające na monitorowanie i konfigurację ochrony dla wszystkich urządzeń w sieci, z możliwością instalacji lokalnej.

Główne funkcje, które musi zapewniać oprogramowanie:

- **Antywirus i antyspyware**: Ochrona przed znanymi oraz nowymi zagrożeniami, zapobieganie rozprzestrzenianiu się wirusów w sieci wewnętrznej.

- **Dwukierunkowy firewall**: Zabezpieczenie przed nieautoryzowanym dostępem do sieci wewnętrznej.

- **System zapobiegania włamaniom (HIPS)**: Kontrola aplikacji i systemu operacyjnego, możliwość ustalania rygorystycznych reguł dla procesów i rejestru systemowego.

- **Kontrola dostępu do urządzeń**: Zarządzanie użyciem urządzeń zewnętrznych, takich jak USB, aby zapobiec nieautoryzowanemu dostępowi.

- **Kontrola dostępu do stron www**: Ograniczanie dostępu do określonych witryn internetowych, aby zwiększyć produktywność i bezpieczeństwo. Kategoryzacje stron internetowych przygotowaną przez producenta.

- **Ochrona przed botnetami**: Zabezpieczenie urządzeń przed przyłączeniem do sieci zainfekowanych komputerów.

- **Ochrona przed phishingiem**: Ochrona przed próbami wyłudzenia poufnych informacji przez fałszywe strony internetowe.

- **Zaawansowana analiza zagrożeń w chmurze**: Analiza podejrzanych plików w odizolowanym środowisku chmurowym.

- **Zaawansowane monitorowanie (XDR)**: Monitorowanie aktywności urządzeń w czasie rzeczywistym, umożliwiające szybką reakcję na incydenty.

Centralna konsola do zarządzania instalowana na infrastrukturze serwerowej zamawiającego (maszyna wirtualna przygotowana przez Wykonawcę) – funkcjonalności:

1. **Zarządzanie instalacjami i aktualizacjami**:

- Konsola umożliwia **centralne wdrażanie oprogramowania** na stacjach roboczych, serwerach i urządzeniach mobilnych. Administrator może tworzyć paczki instalacyjne, które są rozsyłane automatycznie do urządzeń.

- **Zarządzanie aktualizacjami** zapewnia możliwość ustalania harmonogramów aktualizacji oraz testowania nowych wersji na wybranych urządzeniach, co umożliwia pełną kontrolę nad wdrażaniem poprawek.

2. **Monitorowanie i raportowanie**:

   - Konsola oferuje **monitorowanie w czasie rzeczywistym** stanu ochrony wszystkich urządzeń w sieci. Administrator otrzymuje alerty o zagrożeniach, błędach instalacji i stanie bezpieczeństwa.

   - **Zaawansowane raporty** obejmują wykryte zagrożenia, incydenty bezpieczeństwa oraz szczegółowe informacje o skanowaniach i aktywności systemu. Raporty są eksportowalne w formatach CSV lub PDF.

3. **Zarządzanie politykami bezpieczeństwa**:

   - Możliwość definiowania i wdrażania **polityk bezpieczeństwa** obejmujących ustawienia związane z ochroną antywirusową, firewallem, kontrolą dostępu do stron internetowych i zarządzaniem urządzeniami.

   - **Rygorystyczne reguły bezpieczeństwa** pozwalają na konfigurowanie dostępu do urządzeń zewnętrznych (np. USB), a także aplikacji i procesów systemowych.

4. **Reakcja na incydenty**:

   - Konsola umożliwia szybkie działania w przypadku incydentów bezpieczeństwa, takich jak **blokowanie zainfekowanych urządzeń** i izolacja zagrożeń. Zapewnia także możliwość natychmiastowej kwarantanny podejrzanych plików.

- Funkcja **automatycznych powiadomień** wysyła alerty do administratora o krytycznych incydentach, z możliwością integracji z systemami powiadomień (np. e-mail, SMS).

5. **Zarządzanie wieloma platformami**:

   - Konsola obsługuje **zarządzanie urządzeniami na różnych platformach**, takich jak Windows, macOS, Linux oraz Android, z jednego interfejsu.

   - **Skalowalność** konsoli pozwala na łatwe dodawanie nowych urządzeń i monitorowanie zarówno małych, jak i dużych sieci.

6. **Zarządzanie incydentami i raportowanie** (zgodne z NIS2):

   - Konsola musi spełniać wymagania **zgodności z NIS2**, które obejmują raportowanie incydentów w ciągu 24 godzin od ich wykrycia oraz szczegółowe raporty w ciągu 72 godzin. NIS2 wymaga także wdrożenia procedur zarządzania incydentami, obejmujących wykrywanie, analizę i odpowiedź na zagrożenia.

   - **Zarządzanie ryzykiem i analiza zagrożeń**: Konsola powinna wspierać prowadzenie regularnych analiz ryzyka oraz wdrażanie odpowiednich środków zabezpieczających, zgodnie z wytycznymi NIS

Ochrona stacje robocze – Windows:

1. Rozwiązanie musi wspierać systemy Windows 10/Windows 11.
2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
3. Rozwiązanie musi wspierać architekturę ARM64.
4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przedrozpoczęciem procesu instalacji.
6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
7. Skuteczność rozwiązania potwierdzona nagrodami.
8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
11. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
12. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
13. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
14. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
15. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
16. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
17. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
18. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
19. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
20. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 21. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
22. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
23. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
24. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
25. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
26. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
27. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
28. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook.
29. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook.

30. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
31. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
32. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
33. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
34. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
35. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
36. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
37. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
38. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
39. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
40. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
41. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
42. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
43. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
44. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
45. Rozwiązanie musi posiadać dwa wbudowane 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.
46. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
47. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

48. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
49. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
50. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 51. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
52. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. 53. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
54. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
55. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
58. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
59. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
60. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
61. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
62. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
63. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
64. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

65. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d. 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,
e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
69. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
70. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
71. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
72. 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.
73. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
74. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 75. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
76. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
77. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
78. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
79. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
80. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

81. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
82. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
83. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
84. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
85. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
86. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
87. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
88. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
89. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
90. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
91. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
92. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
93. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
94. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
95. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
96. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
97. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
98. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
99. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
100. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.

101. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”
102. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
103. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
104. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
105. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
106. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
107. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
108. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
109. Wsparcie techniczne do programu świadczone w języku polskim przez dystrybutora, autoryzowanego przez producenta programu.

Kontrola dostępu do stron internetowych:

1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli odwiedzanych stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
5. Rozwiązanie musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Podstawowe kategorie w jakie rozwiązanie musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
7. Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
8. Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

Ochrona przed spamem:

1. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
2. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.

3. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
9. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
10. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
11. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall):

1. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
2. Rozwiązanie musi oceniać reguły zapory systemu Windows.
3. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
4. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
5. Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
6. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
7. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
8. Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
9. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.

10. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
12. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
13. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
14. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
15. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
16. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: a. z aplikacją lokalną, którą administrator wskazuje z listy,
b. z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

Kontrola dostępu do stron internetowych:

1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
3. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
4. Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
5. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
6. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
8. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
9. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

Ochrona urządzeń mobilnych opartych o system Android:

1. Rozwiązanie musi wspierać system co najmniej Android 6.0.
2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom.
4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.
5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing".
6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.
9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

1. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.
2. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
3. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
4. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Polityka ustawień:

1. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:

a. połączenie Wi-Fi,
b. GPS,
c. usługi lokalizacyjne,
d. pamięć,
e. roaming danych,
f. roaming połączeń,
g. nieznane źródła,
h. tryb debugowania,
i. komunikacja NFC,
j. szyfrowanie pamięci masowej,
k. urządzenie zrootowane.

Kontrola aplikacji:

1. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
3. Blokowanie aplikacji musi być możliwe w oparciu o:

a. nazwę aplikacji,
b. nazwę pakietu,
c. kategorię sklepu Google Play,

d. uprawnienia aplikacji,
e. pochodzenie aplikacji z nieznanego źródła.

Zabezpieczenia urządzenia:
1. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
a. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
b. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
d. czas, po którym automatycznie nastąpi blokada ekranu,
e. ograniczenie dostępu do kamery wbudowanej w urządzenie.
Aktualizacje modułów:
1. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
2. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin. 3. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:
1. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
2. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.

Dostawa i instalacja oprogramowania:

1. Dostawa:

Oprogramowanie ochrony punktów końcowych, w tym konsola zarządzająca, musi zostać dostarczone jako **maszyna wirtualna**, która będzie wdrożona w środowisku Zamawiającego. Wykonawca odpowiada za dostarczenie gotowego obrazu maszyny wirtualnej, który zostanie zainstalowany na serwerze Zamawiającego, zgodnie z wymogami infrastrukturalnymi (system operacyjny Hyper-V - MSW2019STD).

2. Montaż i konfiguracja:

Montaż obejmuje **kompletną konfigurację** dostarczonego oprogramowania oraz zapewnienie pełnej funkcjonalności systemu w infrastrukturze Zamawiającego. Główne kroki montażu i konfiguracji obejmują:

- **Instalacja konsoli zarządzającej** na maszynie wirtualnej oraz jej integracja z istniejącą infrastrukturą IT Zamawiającego.

- **Konfiguracja polityk bezpieczeństwa** dla:

    - **Stacji roboczych** – dostosowanie ustawień antywirusowych, firewall, systemu zapobiegania włamaniom (HIPS) oraz innych zasad bezpieczeństwa.

    - **Serwerów** – konfiguracja ochrony serwerów plików oraz innych zasobów sieciowych w celu zapewnienia integralności i bezpieczeństwa danych.

- **Uruchomienie systemu powiadomień** – konfiguracja automatycznych powiadomień dla administratora w przypadku wykrycia zagrożeń, naruszeń bezpieczeństwa lub błędów systemowych. Powiadomienia mogą być przesyłane za pośrednictwem e-maila lub SMS, z opcją integracji z systemami do monitoringu sieci.

- **Automatyczne izolowanie zagrożonych urządzeń** – skonfigurowanie mechanizmów automatycznej izolacji urządzeń, które wykryły zagrożenie. System ten zapewnia natychmiastową reakcję na incydenty, ograniczając rozprzestrzenianie się wirusów lub ataków sieciowych w sieci Zamawiającego.

- **Sandboxing** – konfiguracja funkcji izolacji w chmurze, umożliwiającej analizę podejrzanych plików w odseparowanym środowisku, zanim zostaną dopuszczone do dalszej pracy w sieci.

- **Zaawansowane monitorowanie i raportowanie** – włączenie mechanizmów monitorowania, które będą zbierać dane o aktywności w sieci, zagrożeniach oraz stanie zabezpieczeń wszystkich chronionych urządzeń. Konfiguracja raportów, które będą

generowane automatycznie lub na żądanie administratora, z możliwością ich eksportu do formatów takich jak CSV lub PDF.

- **Integracja z infrastrukturą sieciową** – pełna konfiguracja integracji konsoli zarządzającej z istniejącą infrastrukturą sieciową Zamawiającego, obejmująca zarówno stacje robocze, jak i urządzenia mobilne oraz serwery. **Integracja obejmuje również konfigurację systemów uwierzytelniania - Active Directory działające u Zamawiającego**.

- **Testy bezpieczeństwa** – po zakończeniu konfiguracji przeprowadzenie testów funkcjonalnych i bezpieczeństwa, które sprawdzą poprawność działania systemu oraz skuteczność w wykrywaniu i reagowaniu na zagrożenia.

3. Czas montażu:

Cały proces montażu, instalacji i konfiguracji powinien zostać wykonany **maksymalnie w ciągu 8 godzin zegarowych** na miejscu u Zamawiającego. W tym czasie wykonawca będzie odpowiedzialny za:

- Przygotowanie środowiska maszyny wirtualnej.

- Pełną konfigurację polityk bezpieczeństwa i wdrożenie wszystkich funkcjonalności zgodnie z opisem wcześniejszym.

- Uruchomienie systemu powiadomień oraz automatycznej reakcji na zagrożenia.

- Testowanie i weryfikację poprawności działania.

W przypadku napotkania problemów technicznych, wykonawca powinien zapewnić dodatkowe wsparcie w celu rozwiązania wszelkich potencjalnych komplikacji.

3.4 <u>Centralny system logowania zdarzeń sieciowych z UTM – 1 sztuka usługa gromadzenia logów w chmurze</u>

Producent..... Model.....

Opis Przedmiotu Zamówienia

Z uwagi na posiadanie przez Zamawiającego oprogramowania i urządzeń sieciowych rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku chmurowym;.

Poniżej zamawiający określa minimalne wymagania dla systemu.

1.1. **Dysk**

1. System musi obsługiwać:
   a) wspierać powierzchnię dyskową o pojemności minimum 3 TB (dynamiczne w razie potrzeby rozszerzane).

1.2. **Parametry wydajnościowe**

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

1.3. **Logowanie**

1. System musi zapewniać podgląd logowanych zdarzeń w czasie rzeczywistym.
2. System musi zapewniać możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa.

Muszą one obejmować co najmniej:

a) Listę najczęściej wykrywanych ataków;
b) Listę najbardziej aktywnych użytkowników;
c) Listę najczęściej wykorzystywanych aplikacji;
d) Listę najczęściej odwiedzanych stron www;
e) Listę krajów, do których nawiązywane są połączenia;

f) Listę najczęściej wykorzystywanych polityk Firewall;

g) Informacje o realizowanych połączeniach IPSec.

4. System musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Dodatkowo system musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. System musi zapewniać komunikację systemów bezpieczeństwa z systemami, z których przesyłane są logi do systemu centralnego logowania z wykorzystaniem co najmniej z protokołów UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy Zamawiającego.

1.4. **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

1.5. **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

- Malware
- Aplikacje sieciowe

- Email
- IPS
- Traffic
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

1.6. **Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o lokalną bazę.
3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

2.1. Serwisy i licencje

1. System musi być objęty wsparciem do **30 czerwca 2026**.
2. System musi być objęty kopiami zapasowymi realizowanymi codziennie przez Wykonawcę.

2.2 Dostawa i montaż:

1. Instalacja polegająca na podłączenie i gromadzenie logów z posiadanego przez zamawiającego UTM.

Wykonawca jest zobowiązany podpisać z zamawiającym umowę powierzenia danych na gromadzenie i przechowywanie logów.

SŁAWOMIR WASILCZUK
Elektronicznie podpisany przez SŁAWOMIR WASILCZUK
Data: 2024.12.03 10:57:57 +01'00'