Załącznik nr 6 do SWZ - Opis Przedmiotu Zamówienia

na „Dostawę i wdrożenie specjalistycznych urządzeń i oprogramowania niezbędnych do podniesienia bezpieczeństwa systemów teleinformatycznych na potrzeby „Pro-Medica" w Ełku Sp. z o. o.”
Znak Sprawy 3191 / 2022

Przedmiot zamówienia finansowany jest ze środków
pochodzących z Funduszu Przeciwdziałania COVID-19- działania w celu podniesienia
poziomu bezpieczeństwa systemów teleinformatycznych „Pro-Medica" w Ełku Sp. z o. o.”

1. Rozbudowa systemu bezpieczeństwa Szpitala poprzez zakup urządzenia UTM i uruchomienie funkcjonalności klastra wysokiej dostępności UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 4 administratorów do poszczególnych instancji systemu.
System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive z aktualnie posiadanym systemem. 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 musi dysponować minimum:
   a) 18 portami Gigabit Ethernet RJ-45,
   b) 8 gniazdami SFP 1 Gbps,
   c) 4 gniazdami SFP+ 10 Gbps.
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 redundantne zasilanie AC.

Parametry wydajnościowe

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 12 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 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.

Funkcje Systemu Bezpieczeństwa

W ramach dostarczonego systemu ochrony muszą być 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 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. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać 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:
   a) translację jeden do jeden oraz jeden do wielu,
   b) 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.
a) Amazon Web Services (AWS),
b) Microsoft Azure,
c) Google Cloud Platform (GCP),
d) OpenStack,
e) VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) wsparcie dla IKE v1 oraz v2,
   b) obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM),
   c) obsługa protokołu Diffie-Hellman grup 19 i 20,
   d) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,
   e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site,
   f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
   g) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,
   h) obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,
   i) mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   a) pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0,
   b) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta,
   c) producent rozwiązania musi dostarczać 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:
   a) routingu statycznego,
   b) policy based routingu,
   c) 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 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 musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
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 (co najmniej: Facebook, Google Docs, Dropbox) 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:
   a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
   b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
   c) 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.
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. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
   a) ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. 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 min. 48 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 48 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.

Wymagania uzupełniające dot. gwarancji i wsparcia

1. Zamawiający aktualnie posiada urządzenie FortiGate FG200F o numerze seryjnym FG200FT921914398, które zamierza połączyć w klaster z urządzeniem zakupionym w ramach tego postępowania. W celu optymalizacji rozwiązania klastrowego Zamawiający wymaga aby Wykonawca wraz z dostarczanym nowym urządzeniem wyrównał termin gwarancji i wsparcia technicznego dla obu urządzeń dostosowując okres gwarancji i wsparcia urządzenia zakupionego w ramach tego postępowania z urządzeniem już posiadanym przez Zamawiającego

Elementy procesu wdrożenia

1. Instalacja dostarczonego sprzętu (urządzenia UTM) w miejscu wskazanym przez Zamawiającego.
2. Aktywacja urządzenia oraz wykonanie aktualizacji oprogramowania
3. Utworzenie klastra urządzeń z urządzenia dostarczanego i posiadanego przez Zamawiającego - FortiGate 200F
4. Połączenie urządzenia z obecną infrastrukturą sieciową – przyłączenie od strony sieci lokalnej będzie realizowane do przełącznika sieciowego Netgear M4300-24XF za pomocą dwóch portów światłowodowych w standardzie 10GBASE-SR.
5. Sprawdzenie poprawności działania.
6. Przygotowanie dokumentacji powdrożeniowej.
7. Przeprowadzenie instruktażu z praktycznej konfiguracji wg poniższej specyfikacji.

<u>Opis instruktażu</u>

Warsztaty z praktycznej konfiguracji UTM dla nie więcej niż 4 pracowników Zamawiającego. Celem przeprowadzenia warsztatów jest przygotowanie administratorów IT do konfiguracji i bieżącej pracy z systemem UTM. Język szkolenia: polski. Minimalny

zakres szkolenia:

- Konfiguracja trybów pracy urządzenia (transparentny/sniffer lub router/NAT),
- Zarządzanie aktualizacjami oraz backup,
- Budowa i optymalizacja reguł zapory sieciowej,
- Konfiguracja systemu wykrywania włamań (IDS/IPS),
- Monitorowanie wykorzystania aplikacji i blokowanie malware/ransomware,
- Konfiguracja modułu filtrowania stron www,
- Konfiguracja profili antyspam,
- Konfiguracja wielu łączy internetowych WAN,
- Raportowanie i analiza zdarzeń,
- Konfiguracja połączeń tunelowych Site-to-Site IPsec VPN,
- Zarządzanie dostępem zdalnym SSL- VPN,
- Instalacja i konfiguracja aplikacji klienckiej VPN,
- Zarządzanie mechanizmami routingu.

Wymagania dodatkowe dotyczące wdrożenia

1. Zamawiający wymaga, żeby Wykonawca dostarczający i wdrażający rozwiązanie posiadał zatrudnionych na etacie inżynierów posiadających certyfikaty techniczne Producenta dostarczanego rozwiązania: NSE7 lub wyższy.

2. Centralny system logowania, raportowania i korelacji

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 6.0/ 6.5 /7.0, Microsoft Hyper-V 2012 R2/ 2016 / 2019/ 2022, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Interfejsy, Dysk

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności min. 6 TB.

Parametry wydajnościowe

1. System musi być w stanie przyjmować minimum 10 GB logów na dobę.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. 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. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długoczasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

1. W zakresie raportowania system musi zapewniać:
   a) generowanie raportów co najmniej w formatach: HTML, PDF, CSV,
   b) predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników,
   c) funkcję definiowania własnych raportów,
   d) możliwość spolszczenia raportów,
   e) generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

1. W zakresie korelacji zdarzeń system musi zapewniać:
   a) Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany,
   b) Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa,
   c) Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
      i. malware,
      ii. aplikacje sieciowe,
      iii. email,
      iv. IPS,
      v. traffic,
      vi. systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o:
   a) lokalną bazę,
   b) Radius,
   c) LDAP,
   d) PKI.
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.

Gwarancja oraz wsparcie

1. Wsparcie: System musi być objęty serwisem producenta przez okres min. 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Elementy procesu wdrożenia

1. Instalacja dostarczonego oprogramowania jako maszyna wirtualna na dostarczonym w tym postępowaniu (poz. 4) serwerze.
2. Aktywacja licencji oprogramowania.
3. Połączenie posiadanych przez Zamawiającego urządzeń do oprogramowania.
4. Sprawdzenie poprawności działania.
5. Przygotowanie dokumentacji powdrożeniowej.
6. Przeprowadzenie instruktażu z praktycznej obsługi systemu wg poniższej specyfikacji.

Opis instruktażu

Warsztaty z praktycznej obsługi systemu logowania, raportowania i korelacji dla nie więcej niż 4 pracowników Zamawiającego. Celem przeprowadzenia warsztatów jest przygotowanie administratorów IT do bieżącej pracy z systemem logowania. Język szkolenia: polski. Minimalny zakres szkolenia:

- Podgląd logowanych zdarzeń w czasie rzeczywistym,
- Przeglądanie zdarzeń historycznych, budowa filtrów,
- Generowanie raportów,
- Konfigurowanie reguł/powiadomień o zdarzeniach, praca z korelacją logów.

3. Rozszerzenie licencji systemu ochrony antywirusowej o moduł wykrywania oraz reagowania na zagrożenia na stacjach roboczych typu Endpoint Detection & Response (EDR)

Zamawiający posiada licencję ESET Endpoint Security na 340 stanowisk o identyfikatorze publicznym licencji 33C-JPF-KSW. Zamawiający wymaga rozszerzenia powyższej licencji o prawo użytkowania modułu typu Endpoint Detection & Response – konwersji licencji oraz rozszerzenie ochrony do 360 stanowisk wraz ze wsparciem aktualizacji na okres następnych 36 miesięcy.

Wymagania ogólne

Moduł EDR wspiera stacje robocze pracujące na systemach operacyjnych Microsoft Windows minimum w wersji 7/ 8/ 8.1/ 10/ 11.
Konsola centralnego zarządzania modułu EDR pracująca w modelu „on-premise”, zintegrowana z bieżącym rozwiązaniem centralnego zarządzania ochroną antywirusową.
Możliwość instalacji elementów składowych systemu centralnego zarządzania na systemach Linux (m.in. dystrybucjach pochodnych od RedHat Linux).

Funkcjonalności dotyczące modułu EDR

1. Reagowanie w czasie rzeczywistym – izolacja urządzenia od reszty sieci, uruchamianie skanowania na żądanie, zamykanie wszystkich uruchomionych procesów i blokowanie aplikacji na podstawie skrótu kryptograficznego pliku wykonywalnego, restartowanie i wyłączanie stacji roboczej.
2. Przeglądanie i blokowanie modułów na podstawie zróżnicowanych wskaźników, takich jak m.in. skrótów kryptograficznych (hash), modyfikacji rejestru, modyfikacji plików, połączeń sieciowych.
3. Wykrywalnie anomalii i zachowań niebezpiecznych dzięki zasadom wywoływanym

na podstawie zachowań zamiast wykrycia sygnatur lub próbek złośliwego oprogramowania.
4. Rejestrowanie elementów pozwalających na analizę przyczyn problemu – szczegółów zdarzenia, pełnego drzewa procesów każdego potencjalnie złośliwego łańcucha zdarzeń.
5. Zaawansowana klasyfikacja alarmów, która przypisuje incydentom wskaźnik dotkliwości i pozwala administratorowi szybko zidentyfikować urządzenia, które stanowią większe zagrożenie.
6. Dostęp administratora do pełnego zakresu danych na temat wykonywanych modułów obejmujących czas uruchomienia, odpowiedzialnego użytkownika, czas wykonania oraz atakowane urządzenia. Wszystkie dane tego typu przechowywane lokalnie w zasobach sieciowych Zamawiającego.

4. Serwer do wirtualizacji

Lp.	Nazwa komponentu	Wymagane minimalne, parametry techniczne
1	Obudowa	Obudowa rack o wysokości max. 2U z możliwością instalacji min. 12 dysków 3,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
2	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów.
3	Procesor	Zainstalowane dwa procesory (każdy procesor zawierający min. 8 rdzeni), o prędkości bazowej min. 2.8GHz. Procesory posiadające minimum 12MB cache, w pełni obsługujące pamięci DDR4 RDIMM 3200MHz. Wynik wydajności procesora instalowanego w oferowanym serwerze, w systemie dwuprocesorowym, powinien wynosić co najmniej 130 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
4	Pamięć RAM	Minimum 256GB RAM DDR4 RDIMM 3200MT/s, w modułach po 32 GB RAM. Na płycie powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM
5	Zabezpieczenie pamięci	ECC, Memory Mirroring, SDDC, Memory Self-Healing lub PPR, Failed DIMM Isolation, Memory Thermal Throttling, Adaptive Double Device Data Correction (ADDDC), Memory Rank Sparing
6	Pamięć masowa	Zainstalowanych 6 dysków NLSAS o pojemności min. 6TB 3,5” 6.0Gb/s oraz 6 dysków SSD SATA o pojemności min. 960GB 2,5”. Możliwość zainstalowania 2 dysków M.2 SATA, każdy o pojemności min. 120GB Hot-Plug z możliwością konfiguracji RAID 1 za pomocą dedykowanego kontrolera RAID.
7	Kontroler dyskowy	Sprzętowy kontroler dyskowy, posiadający min. 4GB pamięci cache z podtrzymaniem kondensatorowym, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
8	Wbudowane porty	5 x USB z czego nie mniej niż 2x USB 3.0 oraz USB TYP-C na przednim panelu obudowy i 2xVGA z czego jeden na panelu przednim.
9	Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne interfejsy: a) minimum 1 x RJ-45 Ethernet management port, b) minimum 4 zainstalowane interfejsy sieciowe 1Gb Ethernet w standardzie Base-T, c) minimum 2 zainstalowane interfejsy sieciowe 10Gb Ethernet w standardzie Base-T, d) minimum 2 zainstalowane interfejsy sieciowe 10Gb w standardzie SFP+ wyposażone w moduły światłowodowe SFP+ w standardzie 10GBASE-SR.
10	Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200, dedykowana pamięć układu graficznego min. 32MB

11	Sloty PCIe	Minimum 3 sloty PCIe generacji 4.0 x16, w tym minimum jeden slot pełnej wysokości FHHL.
12	Wentylatory	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
13	Zasilanie	Minimum dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza minimum 900W.
14	Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
15	System operacyjny	Wraz z serwerem należy dostarczyć licencję Windows Server 2022 Standard pokrywającą wszystkie rdzenie zainstalowanych procesorów.
16	Diagnostyka	Serwer wyposażony w wyświetlacz LED lub LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie serwera i kodach błędów.
17	Zarządzanie	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; b) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); c) szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; d) możliwość podmontowania zdalnych wirtualnych napędów; e) wirtualną konsolę z dostępem do myszy, klawiatury; f) wsparcie dla IPv6; g) wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; h) możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; i) możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; j) integracja z Active Directory; k) możliwość obsługi przez dwóch administratorów jednocześnie; l) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. m) możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera n) Power-on password
18	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO 9001 lub równoważne oraz ISO 14001 lub równoważne. Serwer musi być serwisowany zgodnie z normą ISO 9001 lub równoważne. Oferowany serwer musi znajdować się na liście Windows

		Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 oraz znajdować się na liście VMware Compatibility Guide – System/ Servers dostępnej na stronie www.vmware.com dla systemu VMware w wersji min. 7.0.
19	Gwarancja	Wymagany jest serwis gwarancyjny min. 36 miesięcy świadczony w trybie 9x5 przez 5 dni w tygodniu z gwarantowanym czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez producenta oferowanego sprzętu lub przez jego autoryzowany serwis. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

5. Urządzenie NAS do archiwizacji

Lp.	Funkcjonalność	Wymagania minimalne
1	Procesor	Procesor ośmiordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.1GHz
2	Obudowa	Rack 19" 3U – wraz z kompletem szyn umożliwiającym zamontowanie w szafie rack
3	Procesor liczba rdzeni	Nie mniej niż 8
4	Pamięć RAM	Minimum 16GB DDR4 ECC
5	Możliwość rozbudowy pamięci RAM do:	Min. 64 GB
6	Całkowita liczba gniazd pamięci	4
7	Liczba zatok na dyski twarde	16
8	Obsługiwane dyski twarde	3.5" SATA HDD oraz 2.5" SATA SSD – Hot Plug Zamawiający wymaga dostarczenia 12 dysków 3.5” o pojemności 12TB każdy o parametrach nie gorszych niż: Prędkość obrotowa: 7200rpm MTBF: min. 2 500 000h Obciążenie roczne: min. 550TB Odporność na wstrząsy (podczas pracy): 70G (czas trwania 2 ms) Drgania (podczas pracy): 0.75G (od 5 do 300Hz) Waga: minimum 720g Wymiary [mm]: 26.1 x 101.85 x 147 Pobór mocy [W]: maks. 7.85 praca / 4.25 bezczynność Gwarancja producenta dysku: 60 miesięcy Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego serwera.
9	Możliwość podłączenia modułu rozszerzającego	Tak

10	Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:	40
11	Porty na karty rozszerzeń	2 x Gen3 x8 PCIe (x8 link)
12	Porty LAN	Wbudowane min. 4 x RJ45 1GbE + 2 x 10GbE RJ-45
13	Porty USB 3.2	min. 2
14	Gniazdo rozszerzenia	min. 2
15	Zasilanie	Redundantny zasilacz o mocy min. 550W
16	Mechanizm szyfrowania sprzętowego	Tak, min. AES-NI
17	Wewnętrzny system plików	BTRFS, EXT4
18	Obsługiwane tryby RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
19	Funkcje backup	Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows (Bare Metal), Linux, maszyn wirtualnych VMware i Hyper-V oraz usług chmur publicznych, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), serwer Apple Time Machine, backup na zewnętrzne dyski twarde, obsługa minimum 1024 migawek na folder udostępniony, obsługa minimum 65000 migawek na cały system
20	Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików
21	Minimum obsługiwane aplikacje/usługi	Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu (min. 2 licencje bezpłatne), możliwość utworzenia klastra wysokiej dostępności z 2 identycznych urządzeń
22	VPN	VPN Server dla min. 60 połączeń
23	Gwarancja producenta na serwer	min. 60 miesięcy

6. Szkolenie w zakresie zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dn. 12.04.2012

Realizacja szkolenia – w trybie stacjonarnym, w siedzibie Zamawiającego
Ilość uczestników – 15 osób

Wytyczne dotyczące zagadnień do zawarcia w programie szkolenia:

1. Omówienie wymagań prawnych:
   a) Krajowe Ramy Interoperacyjności (KRI) – ustawa o informatyzacji podmiotów publicznych realizujących zadania publiczne oraz rozporządzenie KRI
   b) Ustawa o krajowym systemie cyberbezpieczeństwa (KSC);
   c) Przepisy o ochronie danych osobowych - RODO i UODO;
   d) Procesy zarządzania bezpieczeństwem informacji;
2. Odpowiedzialność za bezpieczeństwo informacji w podmiocie realizującym zadanie publiczne, wydajny podział obowiązków w zakresie monitorowania zgodności z KRI
3. Zarządzanie ryzykiem w KRI:
   a) Identyfikacja aktywów chronionych, w tym danych osobowych;
   b) Klasyfikacja aktywów, w tym systemów kluczowych;

c) Metoda identyfikacji ryzyka;
d) Metoda analizy ryzyka;
e) Zasady oceny ryzyka;
f) Kryteria akceptowalności ryzyka RODO i KRI;
g) Formułowanie planów postępowania z ryzykiem.

4. Monitorowanie i audytowanie:
   a) Dobór i pomiar wskaźników bezpieczeństwa;
   b) Określanie wskaźników bezpieczeństwa;
   c) Zasady prowadzania audytu bezpieczeństwa informacji;
   d) Wymagane kompetencje audytorów;
   e) Program audytu.
5. Zarządzanie incydentami KRI i RODO:
   a) Definicja incydentu;
   b) Kryteria incydentów KRI
   c) Zintegrowane zasady obsługi incydentów;
   d) Zasady zgłaszania incydentów.