Załącznik nr 7 do SWZ

Nr sprawy: RI.271.14.2024

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Serwer produkcyjny – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera produkcyjnego.

Wymagania:

2. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 3,5”. Serwer musi posiadać możliwość rozbudowy o 2 dodatkowe wnęki dyskowe na dyski SAS/SATA/NVMe 2.5”.
3. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz możliwością instalacji przedniego panelu zamykanego na klucz, chroniącego dyski przed nieuprawnionym wyjęciem.
4. Płyta główna z możliwością zainstalowania do dwóch procesorów.
5. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
6. Zainstalowane dwa procesory piątej generacji min. 16-rdzeniowe o taktowaniu min. 2GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla dwóch procesorów min. 49000 pkt. Wynik należy dołączyć do oferty.
7. Pamięć RAM min. 128 GB RAM DDR5 RDIMM 5600MT/s, w modułach po 64 GB RAM.
8. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
9. Zabezpieczenie pamięci:
    a. Memory mirroring
    b. ECC
    c. patrol scrubbing
    d. SDDC
    e. memory thermal throttling
    f. ADDDC-SR
    g. PPR
    h. Memory SMBus hang recovery.
10. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
11. Wbudowane porty:
    a. 5 x USB z czego nie mniej niż 1 x USB 2.0, 1 x USB 3.0 TYP-C na przednim panelu obudowy, 2 x USB 3.0 na tylnym panelu obudowy oraz 1 x USB 2.0 na płycie głównej. Złącze USB TYP-C na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS.
    b. 1 x VGA na tylnym panelu obudowy.

   c. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
12. Min. 3 aktywne sloty PCI-E 5.0 x16
13. Możliwość rozbudowy o 5 dodatkowych aktywnych slotów PCI-E.
14. Zainstalowane i w pełni funkcjonalne interfejsy:
    a. min. 1 port RJ-45 Ethernet management port,
    b. minimum 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ Multimode
    c. min. 4 porty 1Gb/s Ethernet w standardzie BaseT,
    d. Porty nie mogą zajmować slotów PCI-E
15. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 6. Kontroler wyposażony w 4GB Cache i podtrzymanie bateryjne. Kontroler powinien posiadać wsparcie dla dysków SAS i SATA.
16. Pamięć masowa:
    a. Zainstalowane 2 dyski serwerowe SSD Read-Intensive o pojemności min. 480 GB każdy nie zajmujące zatok dyskowych 3.5”.
    b. Zainstalowane 4 dyski serwerowe HDD SAS 7.2K o pojemności min. 8 TB każdy.
    c. Zainstalowane 4 dyski serwerowe HDD SAS 10K o pojemności min. 2.4 TB każdy.
17. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
18. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
19. Min. dwa identyczne zasilacze o mocy min. 1600W klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera. W komplecie należy dostarczyć kable zasilające o długości min. 2m.
20. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
21. Możliwość wyposażenia serwera w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:
    a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS
    b. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy
    c. przywracanie konta administratora
    d. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera
    e. wyświetlanie w czasie rzeczywistym temperatury procesorów
    f. konfigurowanie ustawień sieciowych modułu zarządzania.
22. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:
    a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),
    b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer,
    c. zbieranie logów błędów hardware,
    d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,
    e. montowanie wirtualnych napędów,

f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,
g. wysyłanie zawiadomień droga mailową i poprzez SNMP
h. wsparcia dla IPMI, SSH, Redfish
i. wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,
j. nadawanie ról użytkownikom,
k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,
l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.

23. Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    a. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.
    b. tworzenie szablonów instalacyjnych dla systemów operacyjnych.
    c. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.
    d. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.
    e. aktualizacja sterowników i BIOS serwerów.
    f. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
24. Zgodność z normą ISO 9001, ISO 14001, ISO 27001 oraz ISO 50001 lub równoważnymi.
25. Serwer musi posiadać deklaracja CE.
26. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów , Microsoft Windows Server 2022. Certyfikat lub inny dokument potwierdzający zgodność z dostarczanym systemem operacyjnym należy dołączyć do oferty.
27. Razem z serwerem należy dostarczyć system operacyjny o poniższych wymaganiach:

a. Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory, które jest aktualnie wykorzystywane. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania.
b. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
c. Licencja bez ograniczeń czasowych.
d. Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
e. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
f. Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;

g. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;
h. Praca w roli klienta domeny Microsoft Active Directory;
i. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
j. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
k. Zawarta możliwość uruchomienia roli serwera DNS;
l. Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
m. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
n. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
p. Zawarta możliwość uruchomienia roli serwera stron WWW;
q. Zawarta funkcjonalność szyfrowania dysków;
r. Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
s. W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;
t. W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
u. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
v. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
w. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
x. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
y. Obsługa zdalnego pulpitu;
z. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
aa. Obsługa PowerShell 4.0;
28. Razem z serwerem należy dostarczyć 40 licencji dostępowych na urządzenia jeśli oprogramowanie systemu operacyjnego takich licencji wymaga.
29. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
30. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.

31. Razem z serwerem należy dostarczyć oprogramowanie do monitorowania infrastruktury IT, który zapewni kompleksową kontrolę nad zasobami sieciowymi, serwerami,

aplikacjami oraz usługami IT. Oprogramowanie ma zapewnić pełne wsparcie dla operacji IT, wczesne wykrywanie problemów, automatyzację zadań oraz zapewnienie wysokiej dostępności i wydajności infrastruktury. System musi być dostarczony z licencją bezterminową dla 30 hostów/adresów IP o poniższej funkcjonalności:

a. Monitorowanie serwerów i urządzeń sieciowych:
   i. Możliwość monitorowania różnorodnych systemów operacyjnych (Windows, Linux, Unix).
   ii. Obsługa monitorowania urządzeń sieciowych (routery, switchy, firewalle).
   iii. Monitorowanie zasobów fizycznych (CPU, pamięć, dyski twarde).
b. Monitorowanie aplikacji i usług:
   i. Monitorowanie dostępności i wydajności aplikacji webowych oraz baz danych.
   ii. Wsparcie dla monitorowania aplikacji chmurowych (AWS, Azure, Google Cloud).
   iii. Możliwość monitorowania usług takich jak HTTP, HTTPS, FTP, SMTP, DNS itp.
c. Monitorowanie użytkowników i aplikacji www:
   i. Realizacja automatycznych testów pracy użytkownika w aplikacji www
   ii. Monitorowanie wydajności aplikacji z perspektywy użytkownika końcowego.
   iii. Kontrola międzyczasów podstron/kroków scenariusza pracy użytkownika aplikacji www.
d. Alertowanie i powiadomienia:
   i. Definiowanie progów alarmowych i automatyczne powiadamianie (e-mail, SMS, powiadomienia PUSH).
   ii. Możliwość konfiguracji alertów w zależności od krytyczności incydentu.
   iii. Integracja z systemami zarządzania incydentami (ITSM).
   iv. Eskalacja powiadomień
e. Raportowanie i analiza danych
   i. Generowanie raportów dotyczących dostępności, wydajności oraz wykorzystania zasobów.
   ii. Wizualizacja danych w postaci wykresów i dashboardów.
   iii. Możliwość eksportu raportów do formatów takich jak PDF, CSV.
   iv. Tworzenie i modyfikacja raportów za pośrednictwem interfejsu WWW bez konieczności instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash itp.).
   v. Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów według zdefiniowanego harmonogramu, możliwość generowania raportów

dostępności (wg hostów lub usług), raportów SLA (wg hostów lub usług), raportowanie incydentów, awarii itp., raportowanie wydajności sieci, zapis raportów do plików PDF, okresowe wysyłanie raportów e-mailem do wskazanych użytkowników, powiadomienia e-mail o incydencie, zapis zdefiniowanych parametrów raportów celem późniejszego wywołania.

f. Automatyzacja i orkiestracja
   i. Automatyczna konfiguracja nowych urządzeń
   ii. Automatyczne wykonywanie skryptów w odpowiedzi na zdarzenia.
   iii. Integracja z narzędziami do zarządzania konfiguracją (Ansible, Puppet, Chef).
   iv. Możliwość definiowania i uruchamiania zadań uwzględniając harmonogram dni i godzin.

g. Bezpieczeństwo i audyt
   i. Zapewnienie szyfrowanej komunikacji między komponentami systemu.
   ii. Monitorowanie i audytowanie zdarzeń związanych z bezpieczeństwem.
   iii. Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi).
   iv. Wbudowany mechanizm zarządzania użytkownikami systemu.
   v. Możliwość tworzenia grup użytkowników.
   vi. Historia danych statystycznych.
   vii. Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
   viii. Audyt pracy uzytkownika w systemie

h. Integracje i API
   i. Otwarte API umożliwiające integrację z innymi systemami.
   ii. Wsparcie dla integracji z popularnymi narzędziami do zarządzania IT (np. ServiceNow, Jira).
   iii. Natywna integracja z systemami do centralnego gromadzenia logów i analizy zdarzeń opartymi o architekturę Elasticsearch, Opensearch
   iv. Natywna integracja z systemami klasy SOAR
   v. Możliwość korzystania z webhooków do przesyłania danych w czasie rzeczywistym.
   vi. Możliwość konfiguracji oprogramowania poprzez stronę www oraz programistyczne, udokumentowane API.

i. Interfejs użytkownika
   i. Interfejs graficzny do wizualizacji struktury sieci.

ii. Interfejs graficzny do wizualizacji poszczególnych wybranych parametrów urządzeń.

iii. Przyjazny i intuicyjny interfejs webowy dostępny z poziomu przeglądarki.

iv. Możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu oraz dowolnej konfiguracji składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget'ów.

v. Możliwość tworzenia wielu dashboardów

vi. Możliwość tworzenia dashboardów prywatnych jak i współdzielnych pomiędzy innymi użytkownikami aplikacji

vii. Możliwość tworzenia dashboardów typu iFrame - będącymi oknem aplikacji zewnętrznych

viii. Możliwość tworzenia własnych dodatków do dashboardów w formie obietków programistycznych typu Widget. Aplikacja musi wspierać dodawanie własnych rozszerzeń do dashboardów.

ix. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień push.

x. Możliwość tworzenia i zapisywania filtrów dla monitorowanych urządzeń i ich parametrów

xi. Możliwość wykorzystania filtrów podczas tworzenia dashboardów

j. Monitorowanie specyficznych parametrów i elementów infrastruktury:

i. Monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałych parametrów działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta).

ii. Możliwość monitorowania aplikacji i procesów o dynamicznym zachowaniu.

iii. Możliwość monitorowania min. krytycznych elementów infrastruktury, aplikacji, usług sieciowych, protokołów sieciowych, wskaźników systemowych, infrastruktury sieciowej, portów.

iv. Możliwość śledzenia parametrów takich jak:

(a) Telnet na wybrany port - nasłuch na porcie,

(b) Ping dostępność urządzenia,

(c) Odczyt, przetwarzanie i generowanie alertów z pułapek SNMP,

(d) Poprawne działanie serwera DHCP,

(e) Poprawne działanie serwera czasu NTP,

(f) Zajętość danych na poszczególnych partycjach,

(g) Zajętość RAM,

(h) Obciążenie systemu,

(i) Obciążenie dysków,

(j) Ilość zalogowanych użytkowników,

(k) Ilość procesów,

(l) Obecność procesów w systemie,

(m) Synchronizacja dysków programowego RAID,

(n) Synchronizacja dysków sprzętowego RAID,

(o) Kontrola parametrów polecenia VMSTAT,

(p) Obecność SSH.

v. Możliwość śledzenia parametrów monitoringu systemu poczty:

(a) Poprawne działanie serwera SMTP,

(b) Poprawne działanie serwera POP3,

(c) Poprawne działanie serwera IMAP,

(d) Ilość listów w kolejkach serwera Postfix.

vi. Możliwość śledzenia parametrów monitoringu DNS:

(a) Poprawne działanie DNS,

(b) Rozwiązywanie zadanych domen na adresy IP,

(c) Parametry serwerów WWW,

(d) Poprawne działanie serwera WWW,

(e) Kontrola występowania oczekiwanych treści na stronie,

(f) Czas odpowiedzi serwera WWW.

vii. Możliwość śledzenia parametrów monitoringu bazy danych:

(a) Poprawna praca bazy,

(b) Kontrola stanu synchronizacji baz,

(c) Zajętość przestrzeni danych.

viii. Możliwość śledzenia parametrów DRBD i HEARTBEAT:

(a) Poprawne działanie klastra,

(b) Poprawne działanie replikacji danych.

ix. Możliwość śledzenia parametrów macierzy dyskowych:

(a) Analiza statusów ogólnych urządzenia,

(b) Analiza dysków urządzenia.

k. Dodatkowe Elementy Infrastruktury Informatycznej do Monitorowania
   i. Monitorowanie zasobów wirtualnych (maszyny wirtualne, hypervisory).
   ii. Monitorowanie infrastruktury kontenerowej (Docker, Kubernetes).
   iii. Monitorowanie systemów backupowych i urządzeń magazynujących.
   iv. Monitorowanie systemów IoT i urządzeń edge computing.
   v. Monitorowanie systemów SCADA i przemysłowych systemów sterowania.
   vi. Monitorowanie infrastruktury zasilania (UPS, generatory).
   vii. Monitorowanie systemów HVAC (Heating, Ventilation, and Air Conditioning).

l. Architektura Systemu
   i. System musi działać w modelu klient-serwer.
   ii. System pracuje pod kontrolą środowiska systemu operacyjnego Open Source.
   iii. Możliwość wdrożenia systemu zarówno on-premises, jak i w chmurze.
   iv. Wsparcie dla skalowalności poziomej i pionowej.
   v. System musi wspierać architekturę wysokiej dostępności dla każdej warstwy systemu.
   vi. System musi umożliwić rozbudowę, pozwalającą na monitorowanie nieograniczonej wydajnością liczby urządzeń w sieci. Architektura musi umożliwiać rozkładanie obciążenia pomiędzy elementy systemu.

m. Wymagania dotyczące składowania danych

   Możliwość replikacji i backupu danych.

   Gromadzone dane muszą musza być składowane w nierelacyjnej bazy danych.

n. Wymagania dotyczące zgodności

   Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień.

o. Dostępność szczegółowej dokumentacji technicznej w języku polskim dla administratorów systemu.

32. Razem z serwerem należy dostarczyć oprogramowanie do zarządzania uprawnieniami na 25 użytkowników. Oprogramowanie to ma na celu zapewnienie bezpiecznej i efektywnej kontroli nad przydzielaniem i wykorzystywaniem uprawnień administracyjnych, umożliwiając użytkownikom wykonywanie zadań wymagających podwyższonych uprawnień, bez konieczności stałego posiadania pełnych praw administratora. Zakres funkcjonalności:

a. Kontrola dostępu administracyjnego:

   Możliwość przyznawania tymczasowych uprawnień administracyjnych na żądanie użytkownika, na określony czas lub tylko do konkretnej aplikacji.

Funkcjonalność logowania i monitorowania wszystkich działań wykonywanych przy użyciu podwyższonych uprawnień.

Możliwość blokowania dostępu do określonych funkcji systemu operacyjnego oraz aplikacji, nawet po przyznaniu uprawnień administracyjnych.

Uwierzytelnianie wieloskładnikowe (MFA) w celu zapewnienia drugiego poziom kontroli bezpieczeństwa przed udzieleniem uprawnień administratora.

MFA dla użytkowników w dostępie do aplikacji.

b. Zarządzanie uprawnieniami:

   i. Centralne zarządzanie politykami uprawnień, które mogą być dostosowane do różnych grup użytkowników.

   ii. Automatyczne cofanie uprawnień administracyjnych po zakończeniu zadania wymagającego podwyższonych uprawnień.

c. Bezpieczeństwo i zgodność z przepisami:

   i.Zgodność z wymaganiami dotyczącymi audytu bezpieczeństwa oraz przepisami RODO, poprzez szczegółowe rejestrowanie i raportowanie aktywności użytkowników, logowań administratorów i instalacji oprogramowania. Zakres zgodności z RODO musi być opisany w dokumentacji oprogramowania.

   ii.Zgodność z normą ISO 27001. Zakres zgodności z normą ISO 27001 musi być opisany w dokumentacji oprogramowania.

   iii.Zgodność z dyrektywą NIS2. Zakres zgodności z dyrektywą NIS2 musi być opisany w dokumentacji oprogramowania.

   iv.Integracja z istniejącymi systemami bezpieczeństwa IT, w tym z systemami SIEM, w celu monitorowania i analizowania logów.

d. Wsparcie dla różnych platform:

   i. Kompatybilność z Windows 10/11, macOS oraz Linux.

   ii. Możliwość integracji z rozwiązaniami chmurowymi oraz lokalnymi infrastrukturami IT.

e. Interfejs użytkownika:

   i. Intuicyjny i łatwy w obsłudze interfejs dla użytkowników końcowych oraz administratorów IT w języku polskim.

   ii. Możliwość dostosowania interfejsu do indywidualnych potrzeb organizacji.

f. Oprogramowanie powinno być dostarczone w formie agenta instalowanego tylko dla punktów końcowych, lekkie (plik instalacyjny max. 3MB) i łatwe do wdrożenia i nie obciążające zasobów stacji roboczych, centralne i zdalne zarządzanie z dowolnego miejsca z poziomu środowiska hostowanego SaaS klasy korporacyjnej (Microsoft Azure, AWS lub Google Cloud) bez konieczności instalacji aplikacji na lokalnych serwerach.

g. Możliwość zarządzania uprawnieniami ze smartfona za pomocą aplikacji mobilnej na Android i Apple.

h. Rozwiązanie musi działać zarówno online, jak i offline. W przypadku offline zatwierdzenie zmian lub uprawnień musi odbywać się kodem PIN.

i. Możliwość odinstalowania agenta lokalnie na stacji roboczej tylko przy wpisaniu kodu PIN.

j. Jednoczesna obsługa punktów końcowych bez AD, wielodomenowych Active Directory i Azure Active Directory.

k. Dostępność szczegółowej dokumentacji technicznej w języku polskim dla administratorów systemu.

33. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day godziny od momentu zgłoszenia usterki.
    c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.
    e. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
    f. Wymagane oświadczenie producenta oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.
    g. Wymaganie oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
    h. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
        i. możliwość pobierania najnowszego firmware,
        ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
        iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
        iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
34. Zakres prac wdrożeniowych:
    a. Analiza przedwdrożeniowa:
        i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
        ii. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:
    i. Instalacja serwera wraz z oprogramowaniem.
    ii. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
    iii. Integracja z istniejącymi systemami IT zamawiającego.
c. Testy akceptacyjne:
    i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
    ii. Weryfikacja poprawności działania serwera oraz oprogramowania

2. Serwer plikowy – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera plikowego.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z min. 8 zatokami na dyski SATA HDD i SSD o wielkości 3,5 cala oraz 2,5 cala.
2. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack. Maksymalna głębokość urządzenia nie powinna przekraczać 300 mm z uwagi na możliwość instalacji w kompaktowych szafach serwerowych z ograniczoną przestrzenią.
3. Zainstalowany 1 procesor klasy x86 min. 8-rdzeniowy o taktowaniu min. 2.7GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 8 600 pkt. Wynik należy dołączyć do oferty.
4. Pamięć RAM min. 16 GB DDR4 z możliwością rozbudowy do co najmniej 64 GB.
5. Wbudowane porty min. 4 porty USB 3.2
6. Powyższe porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
7. Możliwość instalacji portu HDMI przez PCI-E
8. Min. 2 aktywne sloty PCI-E 3.0 umożliwiające instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe, karty SSD NVMe lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
9. Zainstalowane i w pełni funkcjonalne minimum 2 porty sieciowe Ethernet 2.5GbE RJ45 z obsługą Link Aggregation w celu zwiększenia wydajności transferu i odporności na awarie. Porty nie mogą zajmować slotów PCI-E.
10. Zainstalowane i w pełni funkcjonalne minimum 2 porty optyczne 10GbE SFP+ z modułami optycznymi SFP+ Multimode.
11. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10, 50, 60.
12. Pamięć masowa:
    a. Zainstalowane 2 dyski SSD M2 PCIe NVMe o pojemności min. 1 TB każdy, które umożliwiają korzystanie z technologii buforowania SSD w celu zapewnienia optymalnej wydajności serwera.
    b. Zainstalowane min. 8 dysków HDD SATA o pojemności min. 8 TB każdy.
13. Minimum 3 wentylatory.

14. Min. 2 identyczne zasilacze o mocy min. 300W zainstalowane wewnątrz serwera, pracujące redundantni w celu zapewnienia ciągłości pracy w przypadku awarii jednego z nich.
15. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie danych AES-256, dwustopniowe uwierzytelnianie, zapora sieciowa, oraz ochrona przed atakami typu brute-force.
16. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków, portów LAN, portów USB i zasilaniu.
17. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia i zarządzania kopiami zapasowymi komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność, oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
    a. Kompatybilność z platformami wirtualizacyjnymi: Oprogramowanie musi być kompatybilne z wiodącymi platformami wirtualizacji, w tym VMware vSphere (wersje 6.5 i wyższe) oraz Microsoft Hyper-V (wersje z Windows Server 2016 i wyższe).
    b. Funkcjonalność tworzenia kopii zapasowych:
        i. Oprogramowanie powinno umożliwiać tworzenie pełnych, różnicowych oraz przyrostowych kopii zapasowych maszyn wirtualnych, z możliwością planowania zadań backupu według harmonogramu ustalonego przez administratora.
        ii. Musi wspierać technologię deduplikacji, co pozwala na oszczędność przestrzeni dyskowej przez eliminację zduplikowanych danych w kopiach zapasowych.
        iii. Musi wspierać technologię kompresji, co znacznie skraca czas tworzenia kopii zapasowych, magazynowania i przywracania danych.
        iv. Musi wspierać jednoczesne tworzenie kopii zapasowych wielu maszyn wirtualnych.
        v. Musi oferować funkcję tworzenia kopii zapasowych z komputerów oraz serwerów z systemem Windows.
        vi. Powinno oferować funkcję backupu bezagentowego, umożliwiającą tworzenie kopii zapasowych bez potrzeby instalacji dodatkowego oprogramowania na maszynach wirtualnych.
    c. Zarządzanie kopiami zapasowymi:
        i. Oprogramowanie powinno posiadać centralny interfejs zarządzania, umożliwiający monitorowanie, konfigurowanie i zarządzanie wszystkimi zadaniami backupu z jednego miejsca.
        ii. Musi oferować zaawansowane raportowanie oraz generowanie logów, które ułatwią śledzenie statusu zadań oraz identyfikację potencjalnych problemów.
        iii. Powinno umożliwiać automatyczne usuwanie starych kopii zapasowych na podstawie określonych polityk, co pomoże w efektywnym zarządzaniu przestrzenią dyskową.
    d. Funkcje przywracania danych:
        i. Oprogramowanie musi umożliwiać szybkie i elastyczne przywracanie danych, w tym pełnych maszyn wirtualnych, poszczególnych plików lub katalogów, oraz punktów w czasie (instant recovery).

ii. Powinno wspierać funkcję przywracania na poziomie plików (file-level recovery), umożliwiającą selektywne odzyskiwanie plików bez potrzeby przywracania całej maszyny wirtualnej.

e. Zabezpieczenia i ochrona danych:
   i. Oprogramowanie musi oferować zaawansowane opcje szyfrowania danych zarówno podczas tworzenia kopii zapasowych, jak i w trakcie ich przesyłania (np. szyfrowanie AES-256).
   ii. Powinno wspierać funkcję tworzenia zaszyfrowanych kopii zapasowych, które mogą być przechowywane w bezpiecznych lokalizacjach (np. na serwerach zdalnych lub w chmurze).
f. Wsparcie dla środowisk chmurowych:
   i. Oprogramowanie powinno być kompatybilne z popularnymi usługami chmurowymi, umożliwiając przechowywanie kopii zapasowych w takich środowiskach jak Amazon S3, Microsoft Azure, Google Cloud, itp.
   ii. Powinno oferować funkcję zautomatyzowanego tworzenia kopii zapasowych do chmury, z możliwością szybkiego odzyskiwania danych w przypadku awarii lokalnej infrastruktury.
g. Zamawiający oczekuje licencji na minimum 10 maszyn wirtualnych, z możliwością rozszerzenia w przyszłości. Licencje powinny być wieczyste (perpetual) bez konieczności ponoszenia jakichkolwiek w przyszłości.
h. Wykonawca powinien zapewnić wsparcie techniczne oraz dostęp do aktualizacji oprogramowania przez okres minimum 3 lat od daty dostawy. Wsparcie powinno obejmować pomoc w instalacji, konfiguracji, oraz rozwiązywaniu problemów związanych z działaniem oprogramowania.

18. Zgodność z normą ISO 9001 oraz ISO 14001 lub równoważnymi.
19. Serwer musi posiadać deklaracja CE.
20. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych, oferujący zaawansowane funkcje takie jak: zarządzanie plikami, wirtualizacja, obsługa kontenerów, backup, synchronizacja z chmurą, oraz wsparcie dla wielu użytkowników z zaawansowanymi ustawieniami uprawnień.
21. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
22. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
23. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji, takimi jak Vmware i Hyper-V.
24. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji.
    c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.
    e. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub

równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.

f. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
   i. możliwość pobierania najnowszego firmware,
   ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
   iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,

25. Zakres prac wdrożeniowych:
   a. Analiza przedwdrożeniowa:
      i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
      ii. Opracowanie planu wdrożenia.
   b. Wdrożenie i konfiguracja:
      i. Instalacja serwera oraz oprogramowania oprogramowanie do tworzenia i zarządzania kopiami zapasowymi na serwerze.
      ii. Konfiguracja dysków SSD w RAID 1 oraz dysków HDD w RAID 5.
      iii. Konfiguracja zabezpieczeń.
      iv. Konfiguracja serwera oraz oprogramowania zgodnie z wymaganiami zamawiającego.
      v. Integracja z istniejącymi systemami IT zamawiającego.
   c. Testy akceptacyjne:
      i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
      ii. Weryfikacja poprawności działania serwera wraz z oprogramowaniem.

3. Oprogramowanie do zbierania logów oraz wykrywania incydentów – 1 kpl.

Przedmiotem zamówienia jest dostawa oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT. Oprogramowanie musi być dostarczone w postaci licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania:

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę systemu operacyjnego Open Source.
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi umożliwiać funkcjonowanie bez dostępu do sieci Internet
6. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.

7. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
8. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie
9. System musi zapewniać retencję danych w okresie minimum 365 dni.
10. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
11. Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
12. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
13. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
14. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
15. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
16. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
17. Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.
18. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
19. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
20. Interfejs musi posiadać polską wersję językową.
21. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
22. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
23. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
24. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
25. System musi wspierać mechanizm logowania typu Single Sign On.
26. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
27. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
28. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
29. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.

30. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
31. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
32. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
33. System musi pozwalać na tworzenie parserów z poziomu GUI
34. System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
35. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
36. System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
37. Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).
38. Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.
39. Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
40. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
41. Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
42. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
43. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
44. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
45. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
46. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
47. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
    iv. Syslog,
    v. WEF,
    vi. Flat file,
    vii. Event log,
    viii. WMI,

ix. SNMP trap,
x. XML,
xi. JSON,
xii. JDBC/ODBC
xiii. CSV,
xiv. Email,

Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

48. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
49. System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka
50. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
51. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
52. Operacja z rekordami bazy danych musza być wykonywane jedynie za pomocą składni JSON z wykorzystaniem udokumentowanego API.
53. Wykorzystanie bazy danych musi odbywać się za pomocą REST API z pominięciem wykorzystania klienta typu SQL client.
54. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
55. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
56. System musi posiadać predefiniowany zestaw parserów zdarzeń.
57. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
58. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
59. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
60. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
61. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
62. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
63. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych

64. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
65. System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w Systemie danych.
66. Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
67. System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.
68. System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
69. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
70. System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL.
71. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
72. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
73. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
    a. Wykrycia dowolnej treści w logach,
    b. Wykrycia wystąpienia wartości pola na wybranej liście,
    c. Wykrycia niewystępowania wartości pola na wybranej liście,
    d. Wykrycia zmiany jednego z kilku pól,
    e. Wykrycia zdarzeń występujących z zadaną częstotliwością,
    f. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
    g. Wykrycia zaniku Wiadomości,
    h. Wykrycia nowej wartości pola w zadanym okresie czasu,
    i. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
74. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
75. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
76. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
77. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
78. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
79. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
80. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
81. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.

82. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
83. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
84. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
85. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
86. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
87. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
88. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
89. System musi posiadać wbudowany, dostepny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
90. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
91. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
92. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
93. System musi dostarczony z licencją wieczystą oraz wsparciem producenta na okres minimum 24 miesięcy.
94. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
95. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
96. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
97. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
98. System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.
99. System musi umożliwiać integrację z Mitre ATT@CK.
100. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
101. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
102. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.

103. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
104. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
105. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
106. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
107. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
108. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
109. Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
110. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
111. Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostepnej stronie internetowej producenta.
112. Producent systemu musi umożliwiać rozbudowę oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewnić gotową integrację z systemem SOAR tego samego producenta.
113. Wdrożenie:
    a. Analiza przedwdrożeniowa:
        i. Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT.
        ii. Opracowanie szczegółowego planu wdrożenia.
    b. Instalacja i konfiguracja:
        i. Instalacja i konfiguracja oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT.
        ii. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
        iii. Testy funkcjonalne systemu.
    c. Dokumentacja:
        i. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.
114. Zamawiający wymaga licencji wieczystych z gwarancją i serwisem na okres minimum 24 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
115. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
116. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

4. Klaster HA Firewall z UTM – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania firewall z rozszerzonym pakietem bezpieczeństwa UTM pracującego w klastrze co najmniej Active-

Passive, które zapewnia zaawansowaną kompleksową ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall pracujących w klastrze co najmniej Active-Passive jak i licencje na oprogramowanie UTM na minimum 24 miesiące oraz usługi wdrożeniowe, dlatego wymagane jest uwzględnienie wszystkich elementów w ofercie.

Wymagania:

I. Funkcje modułu Firewall:

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Uruchomienie w formie klastra wysokiej dostępności (HA) co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego agenta na stacjach roboczych użytkowników.
28. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.

29. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
30. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
31. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
33. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
34. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
35. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
36. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
37. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
38. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
39. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

II. Specyfikacja UTM:
1. Firewall musi zapewnić obsługę na poziomie minimalnym: 5.8 Gbps dla pracy w trybie firewall, 1.18 Gbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)
2. Ilość obsługiwanych sieci VLAN: 100
3. Firewall musi obsługiwać 3 500 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 34 000 połączeń na sekundę.
4. Minimalna ilość portów 10/100/1000 BaseT: 8
5. Możliwość rozszerzenia portów o dodatkowe: 4x 1 Gb Copper lub 4x SFP lub 2x SFP+ lub 4x 10Gb multi-speed.
6. Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 75 użytkowników.
7. Minimalna ilość uwierzytelnionych użytkowników: 500.

III. Dostarczony system bezpieczeństwa (UTM) musi zapewniać:
1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

IV. W ramach ochrony przed atakami system musi zapewniać:
1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).

5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

V. W ramach kontroli antywirusowej system musi zapewniać:
1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

VI. W ramach kontroli antyspamowej system musi zapewniać:
1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

VII. W ramach filtrowania zawartości URL system musi zapewniać:
1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

VIII. W ramach kontroli aplikacyjnej system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.

IX. Wymagane funkcje VPN systemu:
1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

X. Zarządzanie:
1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

XI. Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
8. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
9. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
10. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
11. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
12. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
13. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
14. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
15. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
16. System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
17. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
18. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
19. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
20. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
21. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
22. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

XII. Gwarancja:

1. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i muszą być objęte serwisem producenta na terenie RP.
2. Urządzenia objęte minimum 24 miesięcznym okresem gwarancji.
3. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
4. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego rozwiązania, potwierdzające pochodzenie urządzeń z licencjami z oficjalnego kanału dystrybucyjnego producenta.
5. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
6. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
a. możliwość pobierania najnowszego firmware,

b. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
c. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
d. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

XIII. Zakres prac wdrożeniowych:
1. Analiza przedwdrożeniowa:
a. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
b. Opracowanie planu wdrożenia.
2. Wdrożenie i konfiguracja:
a. Instalacja urządzeń firewall wraz z oprogramowaniem UTM.
b. Konfiguracja urządzeń w klastrze co najmniej Active-Passive i oprogramowania UTM zgodnie z wymaganiami zamawiającego.
c. Integracja z istniejącymi systemami IT zamawiającego.
3. Testy akceptacyjne:
a. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
b. Weryfikacja poprawności działania urządzeń firewall pracujących w klastrze Active-Passive oraz oprogramowania UTM.

5. Oprogramowanie EDR – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja oprogramowania EDR na minimum 30 stacji końcowych w formie agentów, które zapewnia zaawansowaną ochronę punktów końcowych (endpointów) w infrastrukturze informatycznej zamawiającego. Oprogramowanie ma na celu ochronę w zakresie minimum: ochrona przed oprogramowaniem ransomware, posiada zaawansowane techniki ochrony przed złośliwym oprogramowaniem malware, exploitami oraz atakami Advanced Persistent Threat (APT), posiada ochronę antytamperową, aktualizuje sygnatury i heurystykę. Zamówienie obejmuje zarówno licencje na oprogramowanie, jak i usługi wdrożeniowe, dlatego wymagane jest uwzględnienie obu elementów w ofercie. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania

1. Ochrona przed zagrożeniami:

a. Ochrona przed znanym oraz nowo wykrytym (zero day) złośliwym oprogramowaniem, ransomware i exploitami.

b. Zabezpieczenie przed zagrożeniami pochodzącymi z różnych wektorów ataku, w tym z sieci, poczty elektronicznej, stron internetowych i urządzeń.

c. Ochrona przed zaawansowanymi zagrożeniami typu APT.

d. Automatyczne aktualizacje zapewniające najnowszą ochronę.

2. Monitorowanie i analiza:

a. Monitorowanie ryzyka na poziomie punktów końcowych.

b. Ciągłe monitorowanie aktywności procesów w chmurze.

c. Przechowywanie danych przez 12 miesięcy w celu retrospektywnej analizy ataków.

d. Graficzne przedstawienie incydentów oraz informacji o cyklu życia zagrożeń dostępne w konsoli webowej.

e. Możliwość eksportu danych dotyczących cyklu życia zagrożeń do analizy lokalnej.

f. System posiada możliwość wybrania jednej lub więcej stacji roboczej, która przeskanuje ich sieć w poszukiwaniu stacji, które nie są obecnie zarządzane przez System.

g. System posiada możliwość alertowania e-mail (z opcjami włącz/ wyłącz dany alert). W skład alertów muszą się znajdywać minimum: detekcja malware, detekcja exploitu, stacja robocza z problemami, stacja robocza bez licencji, znalezienie stacji roboczej nie zarządzanej przez system.

3. Zarządzanie i konfiguracja:

a. Intuicyjny interfejs administracyjny w języku polskim lub angielskim umożliwiający centralne zarządzanie politykami bezpieczeństwa oraz monitorowanie stanu ochrony wszystkich urządzeń w sieci.

b. Centralna, chmurowa konsola zarządzania z możliwością natychmiastowej izolacji zainfekowanych komputerów.

c. Dziedziczenie ustawień między grupami i punktami końcowymi.

d. Możliwość konfigurowania i stosowania ustawień zarówno na poziomie grup, jak i pojedynczych punktów końcowych.

e. Zarządzanie bezpieczeństwem oparte na widokach punktów końcowych oraz dynamicznych filtrach.

f. Przypisywanie ról użytkownikom konsoli zgodnie z predefiniowanymi ustawieniami.

g. Audytowanie aktywności użytkowników oraz dostosowywanie alertów lokalnych.

h. Instalacja oprogramowania za pomocą pakietów MSI, linków do pobrania oraz e-maili wysyłanych do użytkowników.

i. Deinstalacja agenta lokalnie jest chroniona hasłem.

j. Możliwość tymczasowego wyłączenia/ ochrony lokalnie po podaniu hasła.

k. System posiada możliwość wybrania jednej lub więcej stacji roboczej, które będą działać jako pamięć podręczna do przechowywania aktualizacji, instalatorów i wszelkich innych pakietów pobranych z Internetu. Wszystkie inne stacje robocze będą automatycznie

korzystać ze stacji podręcznych, które znajdą w sieci. Jeśli znajdą więcej niż jedną stację podręczną, użyją jednej lub drugiej w zależności od ich dostępności.

l. System posiada możliwość pracy minimum w 3 trybach operacyjnych dla systemów Windows:

◦ Śledzi aktywność każdego programu na komputerach. Nieznane programy mogą być uruchamiane. Złośliwe i potencjalnie złośliwe programy są usuwane.

◦ Śledzi aktywność każdego programu na komputerach. Złośliwe i potencjalnie złośliwe programy są usuwane. Nieznane programy z Internetu, innych komputerów w sieci lub z zewnętrznych dysków są blokowane do czasu ustalenia przez laboratorium producenta, czy są one złośliwym oprogramowaniem. Inne nieznane programy mogą być uruchamiane, gdy są analizowane przez laboratorium.

◦ Śledzi aktywność każdego programu na komputerach. Złośliwe i potencjalnie złośliwe programy są usuwane. Nieznane programy są blokowane, dopóki laboratorium producenta nie ustali, czy są złośliwe.

m. System posiada możliwość pracy w minimum 3 trybach dla systemów Linux:

◦ Śledzenie aktywności każdego programu na stacjach roboczych.

◦ Śledzenie aktywności każdego programu na stacjach roboczych i blokowanie złośliwych i potencjalnie złośliwych programów.

◦ Brak wykrywania złośliwych i potencjalnie złośliwych programów.

4. Integracja i raportowanie:

a. Integracja z narzędziami ConnectWise Automate, Kaseya VSA, N-able N-central oraz N-able N-sight.

b. Dostępność API do integracji zewnętrznej.

c. Generowanie raportów na żądanie oraz według harmonogramu, na różnych poziomach z różnym stopniem szczegółowości.

d. Udostępnienie kluczowych wskaźników wydajności (KPI) oraz dashboardów do zarządzania bezpieczeństwem.

e. Możliwość integracji z innymi narzędziami bezpieczeństwa IT oraz systemami SIEM.

f. Możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku

g. Wsparcie dla automatyzacji zadań administracyjnych i reagowania na incydenty.

5. Zgodność i obsługiwane platformy:

a. Wsparcie dla systemów operacyjnych: Windows, macOS, Linux.

b. Technologia anty-exploitowa zapewniająca ochronę przed wykorzystaniem luk w zabezpieczeniach.

c. Automatyczne wykrywanie niechronionych punktów końcowych.

d. Zabezpieczenie połączeń VPN (wymagana integracja z dostarczonym UTM w postępowaniu) oraz dostęp do sieci Wi-Fi przez punkty dostępu.

e. Usługa o wysokiej dostępności oraz zgodność z certyfikatami platform hosta.

6. Szybka reakcja na incydenty:

a. System musi umożliwiać automatyczne wykrywanie i eliminowanie zagrożeń w czasie rzeczywistym.

b. Powinien zapewniać narzędzia do szczegółowej analizy i raportowania incydentów bezpieczeństwa.

c. Funkcjonalność izolowania zainfekowanych urządzeń w celu zapobiegania dalszemu rozprzestrzenianiu się zagrożeń.

7. Zapewnienie automatycznych i regularnych aktualizacji oprogramowania oraz baz danych z zagrożeniami.

8. Wdrożenie:

a) Analiza przedwdrożeniowa:

- Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia EDR.
- Opracowanie szczegółowego planu wdrożenia.

b) Instalacja i konfiguracja:

- Instalacja i konfiguracja oprogramowania na wskazanych punktach końcowych.
- Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
- Testy funkcjonalne systemu.

c) Dostarczenie pełnej dokumentacji technicznej i użytkowej.

9. Gwarancja: Zamawiający wymaga licencji na okres minimum 24 miesięcy, z możliwością przedłużenia. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

10. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

Elektronicznie podpisany przez
Marcin Wileński
Data: 2024.12.06 11:32:13 +01'00'

BURMISTRZ SZCZUCZYNA

Marcin Wileński

/podpis osoby uprawnionej do reprezentowania Zamawiającego/

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego Cyberbezpieczny Samorząd , Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu Fundusze Europejskie Na Rozwój Cyfrowy 2021-2027 (FERC).