Załącznik nr 10 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

wraz ze wskazaniem wymagań technicznych , użytkowych i serwisowych

odnoszących się do głównych elementów składających się na przedmiot zamówienia

NAZWA ZAMÓWIENIA:

Dostawa sprzętu informatycznego oraz oprogramowania w ramach realizacji projektu „Cyberbezpieczny Samorząd" w Gminie Korycin

ZAMAWIAJĄCY :

Gmina Korycin,
ul. Knyszyńska 2a
16-140 Korycin

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).

1. Serwer produkcyjny – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera do wirtualizacji i monitoringu infrastruktury IT.

Wymagania:

1. 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”.
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz możliwość wyposażenia w przedni panel zamykany na klucz, chroniącym dyski przed nieuprawnionym wyjęciem.
3. Płyta główna z możliwością zainstalowania do dwóch procesorów.
4. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5. Zainstalowane dwa procesory piątej generacji min. 16-rdzeniowe o taktowaniu min. 2GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów w oferowanym serwerze min. 420 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 256GB DDR5 RDIMM 5600MT/s, w modułach po min. 32 GB RAM.
7. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
8. 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.
9. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
10. Wbudowane porty:
    a. 4 porty USB z czego nie mniej niż 1 port USB 3.0 na przednim panelu obudowy, 2 porty USB 3.0 na tylnym panelu obudowy oraz 1 port USB 2.0 na płycie głównej.
    b. Złącze USB TYP-C na przednim panelu, które musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS.
    c. 1 port VGA na tylnym panelu obudowy.
    d. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
11. Minimum 3 aktywne sloty PCI-E 5.0 z czego min. 1 slot x16.
12. Możliwość rozbudowy o 7 dodatkowych slotów PCI-E.
13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,
    b. minimum 4 porty 1Gb/s Ethernet w standardzie BaseT
    c. powyższe porty nie mogą zajmować slotów PCI-E.

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).

14. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 50, 6, 60. Kontroler wyposażony w 4GB Cache i podtrzymanie bateryjne. Kontroler powinien posiadać wsparcie dla dysków SAS, SATA oraz NVMe, jak również powinien wspierać mechanizmy szyfrowania, bądź obsługę dysków SED.
15. Pamięć masowa:
    a. Zainstalowane 2 dyski serwerowe SSD M.2 Read-Intensive o pojemności min. 480 GB każdy. Dyski nie mogą zajmować kieszeni na dyski 3.5".
    b. Zainstalowane 3 dyski serwerowe SSD SATA o pojemności min. 1.92 TB każdy.
    c. Zainstalowane 4 dyski serwerowe HDD SATA 7.2K o pojemności min. 8 TB każdy.
16. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
17. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
18. 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 z zasilaczami należy dostarczyć kable zasilające o długości min. 3m.
19. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
20. 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.
21. 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,

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).

k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,
l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.

22. 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.
23. Razem z serwerem należy dostarczyć Windows Server 2025 Standard na dwie maszyny wirtualne uwzględniając oferowaną ilość rdzeni w serwerze. Opis równoważności licencji oprogramowania:
    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;

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).

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.
bb. Obsługa WiFi i Bluetooth;
cc. Możliwość współdzielenia zasobów GPU między hostami.

24. Dodatkowo należy dostarczyć 20 licencji dostępowych na użytkownika.
25. Wraz z serwerem dostarczone powinno być oprogramowanie dostępu do sieci w infrastrukturze zamawiającego w formie licencji wieczystej na 20 urządzeń końcowych . Oprogramowanie ma na celu zarządzanie, monitorowanie i kontrolowanie dostępu do sieci dla urządzeń końcowych, zarówno przewodowych, jak i bezprzewodowych. Jego zadaniem jest ochrona przed nieautoryzowanym dostępem, zapobieganie zagrożeniom związanym z bezpieczeństwem sieci oraz zarządzanie politykami dostępu dla użytkowników i urządzeń. Wymagania funkcjonalne:
    a. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
    b. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).
    c. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.

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).

d. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
e. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
f. System musi umożliwiać obsługę co najmniej 20 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 2 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
g. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
h. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
i. System musi umożliwiać instalację na maszynie wirtualnej (VM) lub maszynie fizycznej, w tym:
    i. VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
    ii. Maszyny fizyczne - serwery wspierane przez producenta.
j. System musi posiadać funkcjonalność serwerów:
    i. serwera RADIUS dla infrastruktury sieciowej,
    ii. serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    iii. serwera SYSLOG,serwera TACACS+,
    iv. serwera Monitoringu,
    v. serwera DHCP,
    vi. serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    vii. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
k. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
l. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
m. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
n. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.

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).

o. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
p. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
q. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
r. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
s. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
t. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
u. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
v. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
w. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
x. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
y. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
z. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
aa. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
bb. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
cc. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
dd. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
ee. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
ff. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

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).

gg. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
hh. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
ii. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
jj. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
kk. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
ll. System musi posiadać funkcję personalizacji strony gościnnej.
mm. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
nn. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
oo. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
pp. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
qq. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
rr. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
ss. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
tt. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
uu. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
vv. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
ww. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
xx. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
yy. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
zz. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
aaa. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.

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).

bbb. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
ccc. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
ddd. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
eee. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, OpenVPN, Palo Alto, Cisco ASA.
fff. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    i. Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    ii. Czy włączony jest firewall
    iii. Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    iv. Czy jest włączone szyfrowanie dysku systemowego
    v. Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    vi. Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
    vii. Czy w systemie są uruchomione procesy wskazane przez administratora
    viii. Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
    ix. Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
ggg. Wartości klucza rejestru
hhh. Typu wartości: Number, String, Version
iii. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
jjj. System musi współpracować z serwerem tokenów.
kkk. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    i. Microsoft Windows
    ii. Mac OS
    iii. iOS
    iv. Android
lll. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
mmm. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.
nnn. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
ooo. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

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).

i. MAC,
ii. PAP/ASCII,
iii. CHAP,
iv. SNMP,
v. 802.1X.

ppp. Wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.

qqq. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

rrr. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.

sss. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).

ttt. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

i. Tożsamość/Urządzenie końcowe,
ii. Grupa tożsamości/urządzeń końcowych,
iii. Parametry urządzeń końcowych, min: system operacyjny, wersja,
iv. Atrybuty Active Directory,
v. Jednostka organizacyjna tożsamości/urządzeń końcowych,
vi. Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
vii. Grupy urządzeń sieciowych,
viii. Porty urządzeń sieciowych,
ix. Grupy portów urządzeń sieciowych,
x. Jednostka organizacyjna portów,
xi. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
xii. Data, czas ważności polityki,
xiii. Wewnętrzny Captive Portal,
xiv. Metoda autoryzacji.

uuu. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.

vvv. System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

www. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.

xxx. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.

yyy. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.

zzz. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.

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).

aaaa. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
bbbb. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
cccc. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
dddd. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
eeee. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.
ffff. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
gggg. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    i. możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    ii. możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    iii. możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
    iv. usługę OCSP (Online Certificate Status Protocol).
hhhh. System musi posiadać funkcję zintegrowanego serwera DHCP.
iiii. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
jjjj. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
    i. Uruchamianie usługi dla wybranych podsieci,
    ii. Przypisanie ustalonego adresu IP dla adresu MAC.
    iii. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
    iv. Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
    v. Możliwość określania braku dostępu dla wybranych adresów MAC,
    vi. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
    vii. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
    viii. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
    ix. Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
    x. Dokonywanie zmian bez konieczności wyłączania usług.
kkkk. System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

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).

i. Monitoring autoryzacji.
ii. Monitoring dla zdarzeń systemowych.
iii. Monitoring dla zdarzeń DHCP.
iv. Monitoring dla tożsamości.
v. Monitoring dla urządzeń końcowych.
vi. Monitoring dla urządzeń sieciowych.
vii. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
viii. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
ix. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
x. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
xi. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
xii. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
xiii. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
xiv. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
xv. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
xvi. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów WiFi.
xvii. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
xviii. Raport zdarzeń Microsoft Active Directory, minimum:
    A. Logowania,
    B. Logowania do sieci 802.1X

lllll. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
i. wiadomości e-mail,
ii. Syslog,
iii. notyfikacji systemowych.

mmmm. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
i. badanie łączności IP za pomocą ping, traceroute,

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).

ii. tcpdump protokołów RADIUS, TACACS+,
iii. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
A. nazwy użytkownika,
B. adresu MAC,
C. statusu uwierzytelnienia (udana lub nieudana),
D. powodu, jeżeli uwierzytelnienie nieudane,
E. zakresu czasowego, co do dnia, godziny i minuty,
F. wykonanie zdalnego polecenia na urządzeniu sieciowym.

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

26. Razem z serwerem należy dostarczyć oprogramowanie na 20 stacji roboczych do zarządzania uprawnieniami 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:
        i. Możliwość przyznawania tymczasowych uprawnień administracyjnych na żądanie użytkownika, na określony czas lub tylko do konkretnej aplikacji.
        ii. Funkcjonalność logowania i monitorowania wszystkich działań wykonywanych przy użyciu podwyższonych uprawnień.
        iii. Możliwość blokowania dostępu do określonych funkcji systemu operacyjnego oraz aplikacji, nawet po przyznaniu uprawnień administracyjnych.
        iv. Uwierzytelnianie wieloskładnikowe (MFA) w celu zapewnienia drugiego poziom kontroli bezpieczeństwa przed udzieleniem uprawnień administratora.
        v. 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.

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).

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.

27. Zgodność z normą ISO 9001, ISO 14001lub równoważnymi.
28. Serwer musi posiadać deklarację CE.
29. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemu Microsoft Windows Server 2025. Certyfikat lub inny dokument potwierdzający zgodność z dostarczanym systemem operacyjnym należy dołączyć do oferty.
30. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
31. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
32. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i 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 producenta lub autoryzowanego partnera serwisowego producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający

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).

autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.

f. Na wezwanie Zamawiającego wymagane oświadczenie producenta oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.
g. Na wezwanie Zamawiającego 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.

33. Zakres prac wdrożeniowych:
    a. 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.
    b. Testy akceptacyjne:
        i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności..
        ii. Weryfikacja poprawności działania serwera oraz oprogramowania.

2. Serwer do backupu – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera do przechowywania danych.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 12 zatokami na dyski SATA HDD i SSD o wielkości 3,5 cala oraz 2,5 cala. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack.
2. Zainstalowany 1 procesor klasy x86 min. 4-rdzeniowy o taktowaniu min. 2.2GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 5 300 pkt. Wynik należy dołączyć do oferty.
3. Pamięć RAM min. 16 GB RAM DDR4 z możliwością rozbudowy do co najmniej 32 GB.
4. Min. 2 porty USB 3.2. Porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
5. Min. 1 aktywny slot PCI-E 3.0 x8 umożliwiający instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
6. Zainstalowane i w pełni funkcjonalne minimum 4 porty sieciowe Ethernet 1GbE RJ45. Porty nie mogą zajmować slotów PCI-E

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).

7. Możliwość rozbudowy o dodatkowe porty 10GbE za pomocą kart rozszerzeń, w celu zapewnienia wysokiej przepustowości i elastyczności do rosnących wymagań sieciowych.
8. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10.
9. Pamięć masowa:
    a. Zainstalowane 2 dyski SSD M2 PCIe NVMe o pojemności min. 800 GB każdy, które umożliwiają korzystanie z technologii buforowania SSD w celu zapewnienia optymalnej wydajności serwera.
    b. Zainstalowane min. 4 dyski HDD SATA o pojemności min. 16 TB każdy.
10. Minimum 2 wentylatory.
11. Min. 2 zasilacze o mocy min. 350W, zainstalowane wewnątrz serwera, pracujące redundantni w celu zapewnienia ciągłości pracy w przypadku awarii jednego z nich.
12. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie AES-NI.
13. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków i zasilaniu.
14. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia kopii zapasowych i odzyskiwania danych komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność, oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
    a. Zaawansowane funkcje tworzenia kopii zapasowych
    b. Ochrona integralności danych oraz infrastruktury IT
    c. Natychmiastowe odzyskiwanie po awarii
    d. Deduplikacja
    e. Szyfrowanie i kompresja
    f. Statystyki użycia
    g. Wstrzymywanie i wznawianie tworzenia kopii zapasowych
15. Zgodność z normą ISO 9001 oraz ISO 14001 lub równoważnych.
16. Serwer musi posiadać deklaracja CE.
17. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych.
18. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
19. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca na wezwanie Zamawiającego musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
20. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji.
21. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 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. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub

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).

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

e. 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,

22. Zakres prac wdrożeniowych:
    a. Wdrożenie i konfiguracja:
       i. Instalacja serwera oraz oprogramowania oprogramowanie do tworzenia i zarządzania kopiami zapasowymi na serwerze.
       ii. Konfiguracja dysków HDD w RAID 5.
       iii. Konfiguracja zabezpieczeń.
       iv. Konfiguracja serwera oraz oprogramowania zgodnie z wymaganiami zamawiającego.
       v. Integracja z istniejącymi systemami IT zamawiającego.
    b. Testy akceptacyjne:
       i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności..
       ii. Weryfikacja poprawności działania serwera wraz z oprogramowaniem.

3. UPS – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. UPS.

Wymagania:

1. MOC min. 10000VA/10000W
2. Obudowa Rack o wysokości maksymalnej 4U
3. Topologia podwójnej konwersji online
4. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne
5. Czas ładowania akumulatorów: do 4 godzin
6. UPS powinien posiadać zainstalowane wewnętrzne akumulatory
7. Czas podtrzymania systemu dla obciążenia 9000 W– min 11 min przy wykorzystaniu przestrzeni w szafie rack max. 8U dla UPSa i modułu bateryjnego łącznie.
8. Możliwość rozbudowy systemu do uzyskania podtrzymania minimum 55 minut dla w/w obciążenia
9. Ilość gniazd wyjściowych C13: co najmniej 6
10. Ilość gniazd wyjściowych C19: co najmniej 4
11. Gniazda UPS muszą być zaprojektowane są tak, aby pochłaniać zakłócenia i przepięcia spowodowane przez burzę lub wyładowanie atmosferyczne, dzięki czemu zapewnią kompletną ochronę sprzętu i urządzeń.
12. Kolorowy wyświetlacz LCD z intuicyjnym i graficznym interfejsem użytkownika
13. Odchylany panel LCD
14. Automatyczne obracanie ekranu LCD
15. Porty komunikacyjne: USB/RS232/EPO
16. Komunikacja po protokole SNMP oraz http
17. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2
18. Możliwość konfigurowania gniazd krytycznych / niekrytycznych (CL / NCL) za pomocą oprogramowania.

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).

19. Gwarancja min. 24 miesiące
20. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
21. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
22. Zakres prac wdrożeniowych:
    a. Analiza przedwdrożeniowa:
        i. Opracowanie planu wdrożenia.
    b. Wdrożenie i konfiguracja:
        i. Instalacja UPS oraz podłączenie do wskazanych serwerów oraz urządzeń.
        ii. Konfiguracja UPS 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
        ii. Weryfikacja poprawności działania UPS.

4. Oprogramowanie do zbierania i analizy logów z całej infrastruktury IT – 1 kpl.

Przedmiotem zamówienia jest dostawa oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące.

Wymagania:
1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.
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.

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).

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.

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).

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:
    a. Syslog,
    b. WEF,
    c. Flat file,
    d. Event log,
    e. WMI,
    f. SNMP trap,
    g. XML,
    h. JSON,
    i. JDBC/ODBC
    j. CSV,
    k. 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.

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).

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.

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).

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.

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).

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.

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).

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. W komplecie należy dostarczyć oprogramowanie do monitorowania infrastruktury IT. Oprogramowanie ma zapewnić kompleksową kontrolę nad zasobami sieciowymi, serwerami, aplikacjami oraz usługami IT oraz 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.

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).

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

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).

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.

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).

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,
    Poprawne działanie replikacji danych.
ix. Możliwość śledzenia parametrów macierzy dyskowych:
    A. Analiza statusów ogólnych urządzenia,
    B. Analiza dysków urządzenia.
    C. Dodatkowe Elementy Infrastruktury Informatycznej do Monitorowania
x. Monitorowanie zasobów wirtualnych (maszyny wirtualne, hypervisory).
xi. Monitorowanie infrastruktury kontenerowej (Docker, Kubernetes).
xii. Monitorowanie systemów backupowych i urządzeń magazynujących.
xiii. Monitorowanie systemów IoT i urządzeń edge computing.
xiv. Monitorowanie systemów SCADA i przemysłowych systemów sterowania.
xv. Monitorowanie infrastruktury zasilania (UPS, generatory).
xvi. Monitorowanie systemów HVAC (Heating, Ventilation, and Air Conditioning).

k. 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.
l. System musi umożliwić rozbudowę, pozwalającą na monitorowanie nieograniczonej wydajnością liczby urządzeń w sieci. Architektura musi umożliwiać rozkładanie obciążenia pomiędzy elementy systemu.
   Wymagania dotyczące składowania danych
    i. Możliwość replikacji i backupu danych.
    ii. Gromadzone dane muszą musza być składowane w nierelacyjnej bazy danych.
m. Wymagania dotyczące zgodności
    i. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień.
n. Dostępność szczegółowej dokumentacji technicznej w języku polskim dla administratorów systemu.

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).

114. 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. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.
    d. Przeprowadzenie szkolenia w siedzibie klienta z obsługi wdrożonego oprogramowania trwającego minimum 2 godziny.
115. 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.
116. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
117. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

5. Firewall z UTM – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. zapory sieciowej z pakietem bezpieczeństwa UTM które zapewnia zaawansowaną ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall jak i licencje na oprogramowanie UTM na minimum 24 miesiące oraz usługi wdrożeniowe, dlatego wymagane jest uwzględnienie wszystkich elementów w ofercie.

Wymagania

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu,

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).

przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

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).

30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
32. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
43. Urządzenie ma posiadać wbudowany filtr URL.
44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
45. Administrator ma mieć możliwość dodawania własnych kategorii URL.
46. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

blokowanie dostępu do adresu URL,
zezwolenie na dostęp do adresu URL,
blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

47. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
48. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
49. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
50. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
51. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
52. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
53. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

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).

   c. usługę katalogową Microsoft Active Directory.
54. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
55. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
   a. SSL,
   b. Radius,
   c. Kerberos.
56. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
58. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
59. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
60. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
61. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
62. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
63. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   a. równoważenie względem adresu źródłowego,
   b. równoważenie względem połączenia.
64. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
65. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
66. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
67. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
68. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
69. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
70. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
71. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
72. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
74. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
75. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

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).

76. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
77. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
78. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
79. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
80. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
81. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
86. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
87. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
88. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
89. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
90. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
91. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
92. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
93. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
94. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
95. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
96. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
97. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
98. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

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).

99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
100. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
101. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
103. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
105. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
106. Urządzenie ma posiadać usługę DNS Proxy.
107. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
108. Urządzenie musi mieć zaimplementowane Open API
109. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
110. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
111. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
112. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
113. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
114. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
115. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
116. Liczba portów Ethernet 2,5Gbps – min. 8.
117. Liczba portów światłowodowych 1Gbps – min. 1.
118. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
119. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
120. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
121. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
122. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
123. Maksymalna liczba tuneli VPN IPSec – minimum 100.
124. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
125. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
126. Obsługa interfejsów 802.11q (VLAN) – minimum 128
127. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.

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).

128. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
129. Urządzenie nie ma limitu na liczbę użytkowników.
130. Liczba reguł filtrowania – minimum 8 192.
131. Liczba tras statycznego routingu – minimum 512.
132. Liczba tras dynamicznego routingu – minimum 10 000.
133. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
134. Urządzenie musi być wyposażone w moduł TPM.
135. Gwarancja
    a. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także muszą być objęte serwisem producenta na terenie RP.
    b. Urządzenia objęte minimum 24 miesięcznym okresem gwarancji.
    c. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego rozwiązania, potwierdzające pochodzenie urządzeń z licencjami z oficjalnego kanału dystrybucyjnego producenta.
    d. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    e. 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.
136. Zakres prac wdrożeniowych:
    a. Analiza przedwdrożeniowa:
        i. Opracowanie planu wdrożenia.
    b. Wdrożenie i konfiguracja:
        i. Instalacja urządzeń firewall wraz z oprogramowaniem UTM.
        ii. Konfiguracja urządzeń i oprogramowania UTM zgodnie z wymaganiami zamawiającego.
        iii. Integracja z istniejącymi systemami IT zamawiającego wraz z przeniesieniem konfiguracji z obecnie używanych urządzeń.
    c. Testy akceptacyjne:
        i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności..
        ii. Weryfikacja poprawności działania urządzeń firewall oraz oprogramowania UTM.

6. Oprogramowanie antywirusowe – 1 kpl.

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).

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania antywirusowego. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z cyberbezpieczeństwem. Zamówienie obejmuje dostawę licencji na 20 stanowisk na okres minimum 24 miesięcy.

Wymagania:
Administracja zdalna:

a. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
b. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
c. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
d. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
e. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
f. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
g. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
h. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
i. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
j. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
k. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
l. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

2. Ochrona stacji roboczych:
   a. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
   b. Rozwiązanie musi wspierać architekturę ARM64.
   c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
   d. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
   e. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
   f. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

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).

g. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
h. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
i. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
j. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
k. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
l. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
m. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
n. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
o. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
p. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:
    i. zainstalowanych aplikacji
    ii. usług systemowych
    iii. informacji o systemie operacyjnym i sprzęcie
    iv. aktywnych procesów i połączeń sieciowych
    v. harmonogramu systemu operacyjnego
    vi. pliku hosts
    vii. sterowników.

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).

q. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
r. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
s. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
t. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
u. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook.
v. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    i. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    iii. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
w. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
x. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
y. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
z. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
aa. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

3. Ochrona serwerów:
    a. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
    b. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
    c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
    d. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
    e. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
    f. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

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).

g. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
h. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

4. Wymagania dla ochrony serwerów Windows:
   a. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
   b. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
   c. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
   d. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
   e. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
   f. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
   g. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
   h. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
   i. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
5. Wymagania dla ochrony serwerów Linux:
   a. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
   b. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
   c. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
   d. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
6. Ochrona urządzeń mobilnych opartych o system Android:
   a. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
   b. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
   c. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
   d. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
   e. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
      i. usunięcie zawartości urządzenia,

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).

ii. przywrócenie urządzenie do ustawień fabrycznych,
iii. zablokowania urządzenia,
iv. uruchomienie sygnału dźwiękowego,
v. lokalizację GPS.

f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
i. nazwę aplikacji,
ii. nazwę pakietu,
iii. kategorię sklepu Google Play,
iv. uprawnienia aplikacji,
v. pochodzenie aplikacji z nieznanego źródła.

7. Zamawiający wymaga licencji dla 20 stanowisk na okres minimum 24 miesięcy, z możliwością przedłużenia. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
8. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

Zamawiający informuje, że zgodnie z art. 99 ust. 5 ustawy Prawo zamówień publicznych przedmiot zamówienia można opisać przez wskazanie znaków towarowych, patentów lub pochodzenia. W przypadku, gdy w SWZ i OPZ zostały użyte znaki towarowe, patenty lub pochodzenie, oznacza to, że są podane jako przykładowe i określają jedynie minimalne, oczekiwane parametry jakościowe oraz wymagany standard. Zamawiający dopuszcza rozwiązania równoważne opisywanym a wskazane odniesienia należy odczytywać z wyrazami „lub równoważne".

Pod pojęciem „minimalne parametry techniczne, eksploatacyjne, użytkowe, jakościowe i funkcjonalne" Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach technicznych, eksploatacyjnych, użytkowych, jakościowych i funkcjonalnych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Oznacza że wskazaniom tym towarzyszą wyrazy „lub równoważny".

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).

Zgodnie z art. 101 ust. 4 ustawy Prawo zamówień publicznych (Pzp) w sytuacji gdyby w dokumentach opisującym przedmiot zamówienia, zawarto odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp a takim odniesieniom nie towarzyszyło wyrażenie „lub równoważne", to **Zamawiający dopuszcza rozwiązania równoważne opisywanym w każdej takiej normie, europejskiej ocenie technicznej, aprobacie, specyfikacji technicznej, systemowi referencji technicznych. W związku z powyższym należy przyjąć, że każdej: normie, europejskiej ocenie technicznej, aprobacie, specyfikacji technicznej, systemowi referencji technicznych występujących w opisie przedmiotu zamówienia towarzyszą wyrazy „lub równoważne".**

Na każde żądanie Zamawiającego, w tym przed rozpoczęciem stosowania materiałów i urządzeń przewidzianych do zastosowania przy realizacji niniejszego zamówienia, Wykonawca dostarczy Zamawiającemu dokumenty potwierdzające ich dopuszczenie do obrotu i stosowania w budownictwie.

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).