# Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

[Szczegółowy Opis Przedmiotu Zamówienia 1](#_Toc189222764)

[System firewall UTM – 2szt. 3](#_Toc189222765)

[UTM I - 1 szt. 3](#_Toc189222766)

[UTM II - 1 szt. 8](#_Toc189222767)

[Oprogramowanie antywirusowe – dla 80 użytkowników 13](#_Toc189222768)

[Oprogramowanie do backupu – licencja dla 60 użytkowników 19](#_Toc189222769)

[System operacyjny do serwera - 1 sztuka 26](#_Toc189222770)

[Zasilacz awaryjny UPS - 30 szt. 27](#_Toc189222771)

[Dyski do pamięci masowej -10 szt. 29](#_Toc189222772)

[Pamięć masowa I - 2 szt. 30](#_Toc189222773)

[Pamięć masowa II - 1 szt. 31](#_Toc189222774)

[Narzędzie służące wykrywaniu i reagowaniu podejrzanych aktywności na urządzeniach końcowych – dla 34 użytkowników 32](#_Toc189222775)

[Opogramowanie do zarządzania siecią – dla 30 użytkowników 36](#_Toc189222776)

[System do zbierania i analizy logów 44](#_Toc189222777)

[Szkolenia produktowe dla administratora z dostarczonego sprzętu teleinformatycznego 49](#_Toc189222778)

Przewidywany czas realizacji: do 60 dni od dnia podpisania umowy

Miejsce dostawy: Urząd Gminy Garbatka-Letnisko, Ulica Skrzyńskich 1, 26-930 Garbatka-Letnisko

Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, które wskazują lub mogłyby wskazywać na konkretnego producenta/dostawcę – nie stanowi to preferowania konkretnego wyrobu lub producenta/dostawcy, lecz ma na celu jedynie wskazanie cech – parametrów technicznych, użytkowych i jakościowych nie gorszych od podanych w opisie. Należy to więc traktować jedynie jako pomoc w opisie przedmiotu zamówienia.

Jeżeli Wykonawca stwierdzi, że użyte w opisie parametry lub normy krajowe lub przenoszące na normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to oznacza, że mają takie znaczenie, że parametry techniczne tak wskazanych produktów określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy. Wykonawca jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w opisie, również dopuszcza się wykazanie normami równoważnymi w stosunku do tych wskazanych w zapytaniu ofertowym. Na Wykonawcy spoczywa ciężar wykazania "równoważności”.

Wykonawca musi zaoferować spełniające min. takie wymagania i parametry techniczne, jak w opisie przedmiotu zamówienia. Wykonawca może zaoferować produkty o lepszych parametrach. Dostarczone przedmioty zamówienia powinny być fabrycznie nowe, wykonane zgodnie z wymaganiami i normami mającymi zastosowanie do danego wyrobu, wolne od wad, odpowiadać normom jakościowym, określonym we właściwych aktach prawnych, posiadać aktualne aprobaty techniczne, gwarancje producenta oraz winny spełniać wszelkie wymogi przewidziane obowiązującymi przepisami dla tego typu wyrobów.

## System firewall UTM – 2szt.

Parametry techniczne minimum:

### UTM I - 1 szt.

OBSŁUGA SIECI

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.

ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. 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.
5. 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, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

1. 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.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. 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.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. 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.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. 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).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. 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.

OCHRONA ANTYSPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL, Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: PPTP VPN, IPSec VPN, SSL VPN.
3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
7. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator ma mieć możliwość dodawania własnych kategorii URL.
4. 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.
5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
7. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP),
   1. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   2. usługę katalogową Microsoft Active Directory
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL, Radius, Kerberos
4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. 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).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł
9. 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.

ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. 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.
6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: manualnego eksportu do pliku w dowolnym momencie czasu, 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.
18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
4. 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).
5. Urządzenie ma posiadać usługę DNS Proxy.
6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
7. Urządzenie musi mieć zaimplementowane Open API
8. 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.

GWARANCJA I SERWIS

1. Urządzenie ma być objęte min. 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
3. Liczba portów Ethernet 10/100/1000Mbps – min.5.
4. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
5. Przepustowość Firewall (1518 bajtów UDP) – minimum 1Gbps.
6. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1Gbps.
7. Przepustowość filtrowania Antywirusowego – minimum 260Mbps.
8. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 200Mbps.
9. Maksymalna liczba tuneli VPN IPSec – minimum 50.
10. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 5.
11. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20.
12. Obsługa interfejsów 802.11q (VLAN) – minimum 128
13. Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 7 500 nowych sesji/sekundę.
14. Urządzenie nie ma limitu na liczbę użytkowników.
15. Liczba reguł filtrowania – minimum 4 096.
16. Liczba tras statycznego routingu – minimum 512.

Liczba tras dynamicznego routingu – minimum 1 000

### UTM II - 1 szt.

OBSŁUGA SIECI

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.

ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. 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.
5. 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, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

1. 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.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. 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.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS
7. 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.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. 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).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. 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.

OCHRONA ANTYSPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL, Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: PPTP VPN; IPSec VPN, SSL VPN.
3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator ma mieć możliwość dodawania własnych kategorii URL.
4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
5. blokowanie dostępu do adresu URL,
6. zezwolenie na dostęp do adresu URL,
7. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
8. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
9. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
10. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
11. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
12. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
13. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL, Radius, Kerberos.
4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agent
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny
7. 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)
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. 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.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: równoważenie względem adresu źródłowego, równoważenie względem połączenia.
3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. 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.
6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: manualnego eksportu do pliku w dowolnym momencie czasu, 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
18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
4. 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).
5. Urządzenie ma posiadać usługę DNS Proxy.
6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
7. Urządzenie musi mieć zaimplementowane Open API
8. 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.
9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

GWARANCJA I SERWIS

1. Urządzenie ma być objęte min. 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
3. Liczba portów Ethernet 2,5Gbps – min. 8.
4. Liczba portów światłowodowych 1Gbps – min. 1.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.
8. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.
9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.
10. Maksymalna liczba tuneli VPN IPSec – minimum 100.
11. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.
12. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 100.
13. Obsługa interfejsów 802.11q (VLAN) – minimum 128
14. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę.
15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
16. Urządzenie nie ma limitu na liczbę użytkowników.
17. Liczba reguł filtrowania – minimum 8 192.
18. Liczba tras statycznego routingu – minimum 512.
19. Liczba tras dynamicznego routingu – minimum 10 000.
20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
21. Urządzenie musi być wyposażone w moduł TPM

## Oprogramowanie antywirusowe – dla 80 użytkowników

Parametry techniczne minimum:

obejmująca minimum 12 miesięczne wsparcie producenta.

Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

* + Microsoft Windows 10
  + Microsoft Windows 11
  + macOS version 14 "Sonoma"
  + macOS version 13 "Ventura"
  + macOS version 12 "Monterey"
  + macOS version 11 "Big Sur"

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

* Microsoft® Windows Server 2016 Standard
* Microsoft® Windows Server 2016 Essentials
* Microsoft® Windows Server 2016 Datacenter
* Microsoft® Windows Server 2016 Core
* Microsoft® Windows Server 2019 Standard
* Microsoft® Windows Server 2019 Essentials
* Microsoft® Windows Server 2019 Datacenter
* Microsoft® Windows Server 2019 Core
* Microsoft® Windows Server 2022 Standard
* Microsoft® Windows Server 2022 Essentials
* Microsoft® Windows Server 2022 Datacenter
* Microsoft® Windows Server 2022 Core

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

* Microsoft Edge
  + Mozilla Firefox
  + Google Chrome
  + Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

Opis technologii

Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.

1. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
2. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
3. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
4. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
5. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
6. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
7. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
8. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
9. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
10. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
11. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
12. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
13. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
14. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
15. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
17. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
19. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
20. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
21. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
22. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
23. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
24. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
25. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
26. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
27. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
28. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
29. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
30. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
31. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
32. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
34. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
35. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
36. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
37. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
38. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
39. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
40. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
41. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
42. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
43. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
44. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
45. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
46. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
47. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
48. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
49. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
50. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
51. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
53. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
54. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
55. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
56. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
57. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
58. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
59. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
60. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
61. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
62. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
63. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
64. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
65. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
66. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
67. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
68. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
69. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
70. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
71. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
72. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
73. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
74. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
75. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
76. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
77. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
78. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
79. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
80. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
81. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
82. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
83. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
84. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
85. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
86. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
87. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
88. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
89. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
90. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
91. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

Wraz z dostawą zamawiający wymaga wdrożenia zaoferowanego oprogramowania.

Wdrożenie musi być przeprowadzone przez inżyniera posiadającego certyfikat producenta.

W celu potwierdzenia kompetencji wykonawca przedłoży oświadczenie producenta potwierdzające, że wykonawca posiada odpowiednie zasoby do świadczenia usług wsparcia technicznego, a także posiada status partnerski co najmniej Gold - oświadczenie należy dołączyć do oferty. Obsługa techniczna świadczona będzie w języku polskim. Czas reakcji na zgłoszenia Zamawiającego to 1h (60 minut).

## Oprogramowanie do backupu – licencja dla 60 użytkowników

Parametry techniczne minimum:

|  |
| --- |
| Licencja wieczysta, dla 60 użytkowników, obejmujaca minimum 12 miesięczne wsparcie producenta.  Opis ogólny:   1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. 2. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, |
| 1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej |
| 1. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| CAŁKOWITE KOSZTY POSIADANIA   1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
| 1. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
| 1. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji |
| 1. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
| 1. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. |
| 1. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. |
| 1. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. |
| 1. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
| 1. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) |
| 1. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu |
| 1. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API |
| 1. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
| 1. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
| 1. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania |
| 1. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
| 1. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej |
| WYMAGANIA PRO   1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
| 1. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. |
| 1. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru |
| 1. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. |
| 1. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. |
| 1. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. |
| 1. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
| 1. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. |
| 1. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. |
| 1. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. |
| 1. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
| 1. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. |
| 1. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
| 1. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
| 1. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| WYMAGANIA RTO   1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. |
| 1. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| 1. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami |
| 1. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre |
| 1. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. |
| 1. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
| 1. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. |
| 1. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
| 1. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
| 1. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |
| 1. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. |
| 1. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |
| 1. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. |
| 1. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN |
| 1. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle |
| 1. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI |
| 1. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| OGRANICZENIE RYZYKA   1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) |
| 1. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. |
| 1. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |
| 1. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
| 1. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| ŚRODOWISKA FIZYCZNE   1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego |
| 1. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych |
| 1. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE |
| 1. Rozwiązanie musi wspierać system operacyjny macOS |
| 1. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix |
| 1. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) |
| 1. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |
| 1. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów |
| 1. Rozwiązanie musi wspierać backup podłączonych dysków USB |
| 1. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym |
| 1. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) |
| 1. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone |
| 1. Rozwiązanie musi wspierać kontrolę pasma sieciowego |
| 1. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych |
| 1. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN |
| 1. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft |
| 1. Rozwiązanie musi wspierać technologię BitLocker |
| 1. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania |
| 1. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych |
| 1. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych |
| 1. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. |
| 1. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform |
| 1. Rozwiązanie musi wspierać szyfrowanie |
| 1. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne |
| 1. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego |
| 1. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej |
| 1. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| MONITORING   1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
| 1. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| 1. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| 1. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
| 1. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
| 1. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
| 1. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
| 1. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
| 1. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
| 1. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
| 1. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
| 1. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
| 1. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
| 1. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
| 1. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |
| 1. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
| 1. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4 |
| RAPOTOWANIE   1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
| 1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
| 1. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. |
| 1. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V |
| 1. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF |
| 1. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc |
| 1. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach |
| 1. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów |
| 1. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych |
| 1. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych |
| 1. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury |
| 1. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta |
| 1. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. |
| 1. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. |
| 1. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
| 1. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) |
| 1. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.  System operacyjny do serwera - 1 sztuka Oprogramowanie Windows Server 2022 Standard (licencja na 16 rdzeni procesora, wersja OEM)  Warunki równoważności dla systemu Microsoft Windows Serwer 2022 Standard:  1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku  fizycznym I dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą  wbudowanych mechanizmów wirtualizacji.  2. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 10 aktywnych  środowisk wirtualnych systemów operacyjnych.  3. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście  kontenerów.  4. Wsparcie dla rozwiązania Kubernetes.  5. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności  min. 64TB przez każdy wirtualny serwerowy system operacyjny.  6. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.  7. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia  obciążenia serwerów  8. Praca w roli klienta domeny Microsoft Active Directory.  9. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft  Windows Server 2016.  10. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie  Microsoft Active Directory.  11. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z  uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności  stosowania dodatkowych mechanizmów współdzielenia pamięci.  12. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  13. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  14. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik  przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  15. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w  bieżącej pracy.  16. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy  HyperThreading;  17. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich  zawartość.  18. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub  równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  19. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.  20. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych - możliwość uruchomienia aplikacji  działających we wskazanych środowiskach.  21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  22. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym  (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c. umożliwiają kompresję &quot;w locie&quot; dla wybranych plików i/lub folderów,  d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).  23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń  internetowych i intranetowych.  24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa,  pomoc, komunikaty systemowe.  25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez  wybór z listy dostępnych lokalizacji.  26. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń  sieciowych, standardów USB, Plug&amp;Play).  27. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania system  28. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).  29. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.  30. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  31. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez  skrypty.  32. Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server).  33. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego  systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów  dla Zamawiającego. Zasilacz awaryjny UPS - 30 szt. Parametry techniczne minimum:   |  |  | | --- | --- | | **Parametr** | **Wymagania minimalne** | | moc pozorna | min. 850VA | | moc rzeczywista | min. 550VA | | Technologia | VI (line interactive) | | Typ obudowy | wolnostojąca | | **praca sieciowa** |  | | Napięcie wejściowe | 162 ÷ 290 V AC ± 7 % | | Częstotliwość napięcia wejściowego | 40 ÷ 70 Hz ± 1 Hz | | Zakres napięcia wyjściowego | 230 V AC ± 10 % | | Kształt napięcia wyjściowego | Schodkowa aproksymacja sinusoidy / Tak jak na wejściu | | Progi przełączania sieć – UPS | 162 ÷ 290 V AC ± 7 % | | Czas przełączania sieć – UPS | <6ms | | **praca bateryjna** |  | | Napięcie wyjściowe | ~230V ± 10% | | Częstotliwość napięcia wyjściowego | 50 / 60 Hz ± 1% | | Kształt napięcia wyjściowego na pracy bateryjnej | Schodkowa aproksymacja sinusoidy | | Progi przełączania UPS – sieć | ~172 ÷ 280 V ± 7 V | | Przeciążalność | > 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna) | | Zabezpieczenie wyjściowe przeciwzwarciowe | elektroniczne | | Zabezpieczenie wyjściowe przeciążeniowe | elektroniczne | | Czas podtrzymania (P 0,8max/P 0,5max) | minimum 3/8 min | | akumulatory wewnętrzne | minimum 12V5Ah; szczelne, bezobsługowe VRLA | | **pozostałe** |  | | wejście zasilania | Przewód zakończony wtyczką z uziemieniem 16A (PN-E-93201:1997) + uni schucko | | Ilość i typ gniazd wyjściowych | 6x IEC 320 C13 (10A) | | Sygnalizacja | Akustyczno-optyczna | | Dioda syngnalizująca minimum pracę sieciową, bateryjną, niski poziom baterii, przeciążenie, awarię | | Sygnalizacja akustyczna informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu, awarii | | Zimny Start | tak | | Interfejs komunikacyjny | USB HID (kabel w komplecie) | | Automatyczna regulacja napięcia AVR | wymagana | | Waga UPS | do 7kg | | wymiary | nie większe niż: wysokość 189mm; szerokość 100mm; głębokość 325mm | | gwarancja | min 24 miesięcy na elektronikę i 12 miesięcy na akumulatory; | | serwis | Serwis gwarancyjny | | serwis realizowany w systemie door-to-door | | oprogramowanie | jedno uniwersalne oprogramowanie do zarządzania oferowanymi urządzeniami UPS | | oprogramamowanie w języku polskim, tego samego producenta co UPS, do zarządzania i monitorowania pracy UPS | | wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. | | możliwość edycji nazw urządzeń na liście monitorowanych UPSów | | wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer | | certyfikaty producenta (załączyć do oferty) | ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; | | deklaracja CE producenta sprzętu | | karta katalogowa oferowanego sprzętu | | jeżeli oferowana jest rozszerzona gwarancja producenta to wymagane jest dołączenie dokumentu potwierdzającego realizację gwarancji przez serwis producenta (zapis w karcie gwarancyjnej lub oświadczenie producenta) | |
| Dyski do pamięci masowej -10 szt. |

Parametry techniczne minimum:

|  |  |
| --- | --- |
| Pojemność | 16 TB |
| Format | 3.5" |
| Interfejs | SATA III (6 Gb/s) |
| Prędkość obrotowa | 7200 RPM |
| Bufor pamięci | 256 MB |
| Technologia zapisu | CMR (Conventional Magnetic Recording) |
| Średni czas dostępu | 4,16 ms |
| Maksymalna prędkość transferu | 261 MB/s |
| Pobór mocy (operacyjny) | 6,5 W |
| Pobór mocy (spoczynek) | 5,0 W |
| MTBF (Mean Time Between Failures) | 2,5 miliona godzin |
| Wytrzymałość (obciążenie pracą) | 550 TB/rok |
| Gwarancja | 5 lat |
| Wymiary (wys. x szer. x gł.) | 26,1 x 101,6 x 146,99 mm |
| Waga | 670 g |
| Ilość dysków w zestawie | 2 |

### Pamięć masowa I - 2 szt.

|  |  |
| --- | --- |
| Procesor | Jeden 4 rdzeniowy / 4 wątkowy procesor |
| Obudowa | Desktop, 165 x 108 x 232,2 mm |
| Pamięć RAM | 2GB DDR4 (rozszerzalna do 6GB) |
| Ilość obsługiwanych dysków | 2 kieszenie na dyski 3.5" lub 2.5" SATA HDD/SSD |
| Interfejsy sieciowe | 2 x 1GbE RJ-45 |
| Porty USB | 2 x USB 3.2 Gen 1 |
| Wskaźniki LED | Status, LAN, Dysk 1, Dysk 2 |
| Waga | 1,3 kg |
| Zużycie energii | 14,69W (podczas dostępu), 5,04W (hibernacja HDD |
| Obsługa RAID | Basic, JBOD, RAID 0,1, SHRh |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. |
| Licencja na Kamery IP | W zestawie licencja na dwie kamery z możliwością rozszerzenia do 40. |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| Usługi | Serwer VPN  Serwer pocztowy dla kilku domen  Stacja monitoringu  Windows ACL  Integracja z Windows ADS  Firewall  Serwer WWW  Serwer plików  Manager plików przez WWW  Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie  Usługa DDNS  Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID  Snapshot Replication  Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware  Wsparcie dla High Availability |
| Obsługa SSD Cache | Wymagane wsparcie dla SSD Cache |
| Obsługa migawek | Maksymalna liczba migawek folderów współdzielonych: 1 024  Maksymalna liczba migawek systemu: 65 536 |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów |
| Język GUI | Polski |
| Certyfikaty | CE |
| System plików | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) |
| Liczba wolumenów | Do 64 |
| Liczba iSCSI Targetów | Do 128 |
| Liczba iSCSI LUN | Do 256 |
| Liczba kont użytkowników | 2048 |
| Liczba grup | 256 |
| Liczba folderów udostępnionych | 256 |
| Ilość jednoczesnych połączeń | 1500 dla CIFS/AFP/NFS/FTP/WebDAV |
| Zasilacz | Adapter 60W |
| Chłodzenie | 1x FAN 92 mm x 92 mm |
| Gwarancja i serwis | 3 lata gwarancji na NAS |
| Dyski | 2x dysk o pojemności 16TB, prędkość obrotowa na poziomie 7200RPM, gwarancja co najmniej 36 miesięcy, dysk pochodzić musi od tego samego producenta co serwera. |

### Pamięć masowa II - 1 szt.

|  |  |
| --- | --- |
| Procesor | Jeden 2-rdzeniowy /4-wątkowy procesor |
| Obudowa | Tower o wymiarach max. 167 × 200 × 224 mm |
| Pamięć RAM | 4GB pamięci SO-DIMM DDR4 ECC z opcja rozszerzenia do 32GB SO-DIMM DDR4 ECC |
| Ilość obsługiwanych dysków | 4 dysków o maksymalnej pojemności 16TB każdy  2 dyski M.2 NVMe 2280 |
| Interfejsy sieciowe | 2 x Gigabit (10/100/1000); Wsparcie dla Link Agregation. |
| Porty | 2 x USB3.2, 1 x eSATA |
| Wskaźniki LED | Status, HDD1-4, Power on; LAN 1-4 |
| Obsługa RAID | Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6,10 |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. |
| Licencja na Kamery IP | W zestawie licencja na dwie kamery z możliwością rozszerzenia do 40. |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| Usługi | Serwer VPN  Serwer pocztowy dla kilku domen  Stacja monitoringu  Windows ACL  Integracja z Windows ADS  Firewall  Serwer WWW  Serwer plików  Manager plików przez WWW  Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie  Usługa DDNS  Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID  Snapshot Replication  Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware  Wsparcie dla High Availability |
| Obsługa SSD Cache | Wymagane wsparcie dla SSD Cache |
| Obsługa migawek | • Maksymalna liczba migawek folderów współdzielonych: 1 024  • Maksymalna liczba migawek systemu: 65 536 |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów |
| Język GUI | Polski |
| Waga | Do 3 kg |
| Certyfikaty | CE |
| System plików | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) |
| Liczba wolumenów | Do 64 |
| Liczba iSCSI Targetów | Do 128 |
| Liczba iSCSI LUN | Do 256 |
| Liczba kont użytkowników | 2048 |
| Liczba grup | 256 |
| Liczba folderów udostępnionych | 512 |
| Ilość jednoczesnych połączeń | 1000 dla CIFS/AFP/NFS/FTP/WebDAV |
| Zasilacz | 100W |
| Chłodzenie | FAN x 2 92 mm x 92 mm |
| Gwarancja i serwis | 3 lata gwarancji na NAS |
| Dyski | 4x dysk o pojemności 6TB, prędkości oprotowej 5400RPM, posiadających 3 lata gwarancji, dysk pochodzić musi od tego samego producenta co serwera. |

## Narzędzie służące wykrywaniu i reagowaniu podejrzanych aktywności na urządzeniach końcowych – dla 34 użytkowników

Parametry techniczne minimum:

obejmująca minimum 12 miesięczne wsparcie producenta.

Opis techniczny:

System musi być zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Ten sam agent zainstalowany na systemach Windows musi umożliwiać rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Rozwiązanie musi posiadać możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

* Microsoft Windows 10
* Microsoft Windows 11
* macOS version 14 "Sonoma"
* macOS version 13 "Ventura"
* macOS version 12 "Monterey"

Rozwiązanie musi posiadać możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

* Microsoft® Windows Server 2016 Standard
* Microsoft® Windows Server 2016 Essentials
* Microsoft® Windows Server 2016 Datacenter
* Microsoft® Windows Server 2016 Core
* Microsoft® Windows Server 2019 Standard
* Microsoft® Windows Server 2019 Essentials
* Microsoft® Windows Server 2019 Datacenter
* Microsoft® Windows Server 2019 Core
* Microsoft® Windows Server 2022 Standard
* Microsoft® Windows Server 2022 Essentials
* Microsoft® Windows Server 2022 Datacenter
* Microsoft® Windows Server 2022 Core

Wspierane przeglądarki internetowe:

* Microsoft Edge
* Mozilla Firefox
* Google Chrome
* Safari

Rozwiązanie musi posiadać polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie bez restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
   * dostęp do pliku;
   * tworzenie nowego procesu;
   * nawiązane połączenia sieciowe;
   * wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
   * zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
12. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
18. Każda detekcja zawiera co najmniej następujące informacje:
    * Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
    * Data i czas wystąpienia podejrzanych zdarzeń.
    * Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
    * Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
    * Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
    * Poziom ryzyka, określający istotność danej detekcji.
    * Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
19. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
20. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
21. Rozwiązanie musi umożliwiać oznaczanie wygenerowanych detekcji jako błędne.
22. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
23. Rozwiązanie musi posiadać możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
24. Rozwiązanie musi posiadać na dodanie własnego komentarza przy wykrytej detekcji.
25. Rozwiązanie musi możliwiac wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
26. Rozwiązanie musi posiadać na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
27. Rozwiązanie musi posiadać na izolację sieciową komputerów przez administratora.
28. Rozwiązanie musi umożliwiac tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
29. Rozwiązanie musi umożliwiac wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
30. Rozwiązanie musi umożliwiac tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
31. Rozwiązanie musi pozwalac na eksport raportów, w postaci plików PDF.
32. Rozwiązanie musi wspierac dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
33. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
34. Konsola zarządzająca wyposażona w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
35. Rozwiązanie musi umożliwiac wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
36. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
37. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
38. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
39. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami.
40. Dodanie klucza licencyjnego skutkuje aktywowaniem zawartości zakładki obsługującej dany produkt w portalu zarządzającym.

Wdrożenie dostarczonego systemu:

Wraz z dostawą zamawiający wymaga wdrożenie zaoferowanego rozwiązania.

Wdrożenie musi być przeprowadzone przez inżyniera posiadającego certyfikat producenta.

W celu potwierdzenie kompetencji wykonawca przedłoży oświadczenie producenta potwierdzające, że wykonawca posiada odpowiednie zasoby do świadczenia usług wsparcia technicznego, a także posiada status partnerski co najmniej Gold - oświadczenie należy dołączyć do oferty. Obsługa techniczna świadczona będzie w języku polskim. Czas reakcji na zgłoszenia Zamawiającego to 1h (60 minut).

## Opogramowanie do zarządzania siecią – dla 30 użytkowników

Parametry techniczne minimum:

obejmująca minimum 12 miesięczną wsparcie techniczne

Wymagania ogóne:

1. Oprogramowanie musi posiadać interface użytkownika w języku polskim.
2. Wsparcie techniczne mailowe oraz telefoniczne musi byś dostępne w języku polskim.
3. Dane muszą być przechowywane w bazie MS SQL (wersja płatna lub darmowa).
4. System musi posiadać mechanizm automatycznego usuwania danych z audytu oraz monitoringu starszych niż wybraną ilość dni, co zapewni automatyczne pilnowanie wielkości bazy.
5. Moduły systemu muszą być wzajemnie zintegrowane. Korzystanie z tych samych słowników, katalogu użytkowników, informacji o majątku itp.
6. System musi zapewnić możliwość logowania do systemu z różnymi poziomami uprawnień. System musi umożliwić podział bazy danych na homogeniczne całości (możliwość odizolowania np. poszczególnych jednostek organizacyjnych pod względem zarządzania w systemie oraz pracy z wynikami na podstawie uprawnień użytkowników systemu).
7. System musi posiadać opcję automatycznego przypisywania użytkowników do komputerów na podstawie zalogowanego użytkownika na stacji.
8. Musi istnieć opcja podziału komputerów do grup według struktury organizacyjnej, lokalizacji i użytkownika.
9. Musi istnieć opcja przypisania administratora do pewnej grupy komputerów i na tej podstawie system musi zabezpieczyć, by przypisany administrator po zalogowaniu widział wyłącznie dane z przypisanych do niego komputerów.
10. Systemu musi umożliwiać określenie dostępu do poszczególnych części systemu na podstawie uprawnień użytkownika. W zależności od ustawionego poziomu dostępu system musi ukryć odpowiednie elementy interfejsu, np. administrator majątku po zalogowaniu widzi tylko elementy dotyczące majątku.
11. System musi umożliwić integrację z Active Directory - wsparcie wielu domen - dla komputerów oraz osób można ustawić dowolną ilość domen lub kontenerów, które będą synchronizowane.
12. Musi być dostępna opcja cyklicznej synchronizacji użytkowników i komputerów z Active Directory. Po synchronizacji możliwość automatycznego uruchomienia dowolnych poleceń SQL.
13. System musi posiadać natywny sposób instalacji agentów (bez użycia paczek msi lub exe; bezpośrednio z konsoli/strony zarządzania system) i zarazem umożliwiać instalację z paczek msi.
14. System oprócz domyślnego sposobu przesyłania wyników musi umożliwić agentom wysyłanie wyników na serwer FTP.
15. Możliwość pracy systemu w: sieciach rozproszonych, sieciach spiętych VPN-em, w Internecie (za NAT-em).
16. Interface systemu musi umożliwiać eksport wszystkich tabeli oraz raportów do formatów: .csv, .xls lub .xlsx, .html, .pdf, .rtf, .jpeg, .png.
17. System musi posiadać interface webowy dla całego systemu – umożliwiający przeglądanie wyników z audytu oraz monitoringu za pośrednictwem przeglądarki www według definiowanych uprawnień. Dostępna musi być opcja przeglądania wyników z własnego komputera lub z danej jednostki organizacyjnej czy lokalizacji.
18. System musi umożliwiać zapisanie ustawień tabelek, musi istnieć opcja, by zapisać: widoczność, szerokość i kolejność poszczególnych kolumn.
19. Musi istnieć opcja dostosowania głównego menu konsoli zarządzającej. Dodatkowo system powinien posiadać pasek zawierający skróty do najczęściej używanych ekranów systemu.
20. System musi umożliwiać dostosowanie interface (www lub aplikacja natywna) za pomocą tematów (schematy kolorów elementów interface).
21. System musi umożliwiać tworzenie kopii zapasowej bazy danych oraz jej odtwarzanie bezpośrednio z konsoli zarządzającej.
22. W związku z rozporządzeniem RODO system musi umożliwiać monitorowanie modyfikacji w katalogu osób oraz anonimizację danych użytkowników.

Synchronizacja z Active Directory:

1. System musi umożliwiać pobieranie danych z wielu domen - dla komputerów oraz osób można ustawić dowolną ilość domen lub kontenerów, które będą synchronizowane.
2. System musi umożliwiać automatyczne zmiany stanu komputerów usuniętych z AD. Na przykład: jeżeli komputer (jako obiekt) zostanie wyłączony w AD lub zostanie skasowany z domeny - automatycznie zostanie zmieniony stan na „Usunięty” (lub podobny). Ta funkcjonalność musi być opcjonalna.
3. System musi mieć opcję cyklicznego pobierania i zapisywania nowych osób oraz komputerów z AD.

Audyt

1. System musi umożliwiać przeprowadzenia audytu na komputerach z systemami Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows 2008 R2 Server, Windows 2012 Serve, Windows Serwer 2016, Windows Serwer 2019, Windows Serwer 2022.
2. System musi umożliwiać audyt stacji z system Linux – wsparcie dystrybucji takich jak Debian, Ubuntu, RHEL, Centos oraz wszystkich ich pochodnych. Skan musi wykrywać oprogramowanie zainstalowane z paczek, sprzęt, daemony (usługi) oraz pliki danych. Agent musi umożliwiać uruchamianie audytu wg ustawionego harmonogramu.
3. Musi istnieć opcja, by w ramach audytu wyświetlić ankietę użytkownikowi komputera, zdefiniowaną przez administratora. Wyświetlanie/niewyświetlanie musi być konfigurowalne.
4. System musi posiadać opcję audytowania komputerów za pośrednictwem zewnętrznego nośnika (pendrive) lub wersji przenośnej agenta. Chodzi o audyt komputerów niepodłączonych do sieci lub w sieciach odseparowanych.
5. Agent musi zebrać szczegółowe dane na temat komputera i jego podzespołów (procesorów, pamięci, płyty głównej, dysków twardych, nośników danych itp.) wraz z numerami seryjnymi (lub możliwość ręcznego dopisania numerów seryjnych).
6. System musi automatycznie wykrywać typ komputera podczas audytu – i potem wyraźnie rozgraniczać stacjonarne, przenośne, serwery oraz wirtualne komputery.
7. Podczas audytu musi być wykrywana wersja systemu operacyjnego wraz z kluczem licencyjnym i numerem seryjnym.
8. System musi dokładnie wykrywać oprogramowanie zainstalowane na komputerze. Nie zależnie od tego, czy program został zainstalowany przez użytkownika (do profilu użytkownika), czy przez administratora. Niezależnie od tego, czy program został skopiowany (np. kopia „Program Files” ze starego komputera), czy zainstalowany z paczki msi lub pliku exe. W tych wszystkich wypadkach program musi się pojawić na liście wykrytego oprogramowania.
9. MS Office musi być wykryty wraz z kluczem licencyjnym, jeżeli jest używany dla tej wersji Office/Microsoft 365.
10. System musi umożliwiać dostosowanie wyświetlanej szczegółowości wersji dla każdego programu (np. możliwość grupowania 4.x lub 4.1.x itd.).
11. System musi umożliwić zbieranie informacji (nazwa, ścieżka, wielkość pliku) na temat wszystkich plików na dysku. Musi umożliwiać administratorowi zdefiniowanie rozszerzeń plików, które będą brane pod uwagę podczas skanowania.
12. System musi wyświetlać ścieżki do plików deinstalatorów wszystkich programów instalowanych z plików exe.
13. System musi posiadać ekran, na którym można sprawdzić dokładne nazwy aplikacji oraz producenta tak, jak są zapisane w „Dodaj i usuń programy” w systemie Windows.
14. System musi posiadać agenta na urządzenia z systemem Android. Musi on umożliwiać zebranie danych na temat zainstalowanych programów oraz informacje o sprzęcie. Audytowanie urządzeń z Androidem nie może wymagać dodatkowych licencji w systemie.
15. Musi istnieć możliwość przeglądania wyników z audytu za pośrednictwem przeglądarki www. Dostępne muszą być raporty zbiorcze oraz szczegółowe wyniki z poszczególnych komputerów.

Raportowanie

1. System musi posiadać raport wyświetlający wkrótce wygasające licencje i gwarancje.
2. Muszą być dostępne raporty wyświetlające zbiorczo znalezione oprogramowanie z możliwością wyświetlania danych statystycznych dla poszczególnych jednostek organizacyjnych lub lokalizacji (np. odpowiedź na pytanie: Ile mamy Office w dziale informatyki?).
3. Muszą istnieć raporty wyświetlające, do których programów została przypisana licencja), a które jej nie posiadają.
4. System musi wyświetlać ilość wolnego miejsca na dyskach komputerów. Powinna być dostępna informacja o ilości wolnego miejsca w procentach i GB.
5. Muszą istnieć raporty wyświetlające nazwę, rozmiar oraz dokładną lokalizację (ścieżka dostępu) plików danych.
6. System musi umożliwiać automatyczne porównywanie zmian pomiędzy stanem aktualnym a poszczególnymi audytami dla oprogramowania i sprzętu.
7. System musi umożliwiać szybkie fulltextowe wyszukiwanie we wszystkich tabelach oraz obliczeń statystycznych w kolumnach.
8. System musi posiadać raporty graficzne. Minimum to 5 różnych rodzajów danego raportu. Raporty graficzne muszą dotyczyć danych sprzętowych (np. wykaz rodzajów procesorów w formie graficznej) oraz statystyk oprogramowania (np. top X najczęściej występujących programów).
9. W oprogramowaniu musi istnieć opcja tworzenia dokumentów dotyczących przekazania majątku, np.: protokół przekazania komputera, karta majątku itp.
10. Baza SQL musi być utworzona logicznie, nazwy tabelek muszą sugerować ich zawartość a relacje pomiędzy nimi muszą być oczywiste lub udokumentowane przez producenta. System musi mieć możliwość tworzenia i uruchamiania własnych raportów – zapytań SQL bezpośrednio z programu.
11. System musi posiadać wbudowany designer raportów, możliwość pracy z szablonami raportów.
12. System powinien posiadać dashboard – zestaw raportów przeglądowych. Najważniejsze informacje dotyczące oprogramowania, licencji, sprzętu, majątku, na jednym ekranie.
13. System musi posiadać raport dotyczący majątku w organizacji. Ma on umożliwiać statystyczny widok posiadanego majątku. Zestawienia w postaci wykresów, tabelek lub innych elementów muszą umożliwienie odpowiedzi na pytania typu „Ile mamy drukarek w organizacji?”.

Licencjonowanie i baza wzorców

1. System musi umożliwiać zarządzanie posiadanymi licencjami – bieżące śledzenie licencji i porównywanie zakupionych licencji z użytkowanymi.
2. Musi istnieć możliwość wprowadzania licencji Upgrade, czasowych, ewidencja licencji CAL, MOLP, OEM.
3. System musi mieć opcję przypisania różnych programów lub wielu wersji programu do jednej licencji. Licencje są automatycznie przeliczane wg ustawionego priorytetu (np. pod jedną pozycję wpisujemy 10szt. licencji systemu operacyjnego a licencja może obowiązywać dla Windows 10 oraz Windows 11).
4. Zarządzanie licencjami musi umożliwiać automatyczne przypisywanie oraz odbieranie. Dla multilicencji lub licencji retailowych można wykorzystać oprócz automatycznego przypisywania również automatyczne odbieranie. Jeżeli program zostanie usunięty z komputera, licencja wróci do puli wolnych licencji. Jeżeli program zostanie zaktualizowany to, jeżeli licencja na to pozwala, zostanie przeniesiona na aktualną wersję programu.
5. Identyfikacja zainstalowanego oprogramowania na podstawie własnej bazy wzorców aplikacji, programów – system sam natychmiast automatycznie rozpoznaje każdą nową wersję znanego oprogramowania bez ręcznego uzupełniania wpisu w bazie.
6. System musi oferować bezterminowe uprawnienia do aktualizacji bazy wzorców aplikacji, programów (bez konieczności wykupienia wsparcia, subskrypcji, abonamentu itp.).
7. System musi posiadać rozpoznawanie oprogramowania na podstawie wzoru generowanego za pomocą zdefiniowanych reguł (automatyczne wykrycie i rozpoznanie nowej wersji wcześniej zidentyfikowanego programu).
8. Musi istnieć opcja edycji bazy wzorców – tworzenie reguł, wyjątków.

Zarządzanie majątkiem

1. System musi automatycznie wykrywać typ komputera (stacjonarny, przenośny, wirtualny, …).
2. System musi umożliwiać ewidencjonowanie dowolnego sprzętu elektronicznego (skaner, drukarka, pendrive, switch, komórka itd.), ale również np. szafa, biurko, samochód, ...
3. System musi umożliwiać zachowanie danych dotyczących wycofanego komputera w bazie danych nie zajmując licencji systemu audytującego.
4. System musi posiadać funkcję importu sprzętu do programu z pliku csv.
5. W module majątku musi istnieć opcja dodania własnych pól dla obiektu majątku.
6. System musi umożliwiać rejestrowanie napraw sprzętu.
7. System powinien umożliwiać przeglądy majątku - wykonywanie cyklicznych działań, takich jak regularne przeglądy, testy czy serwis. System ma ostrzegać o zbliżających się przeglądach za pośrednictwem komunikatów lub wysyłając maila pod wskazane adresy.
8. Operacje na majątku muszą umożliwiać wykonywanie ich na wielu pozycjach na raz. Zbiorcze działania muszą umożliwiać szybkie przenoszenie do magazynu, zmiany stanu, przeniesienia pomiędzy jednostkami, lokalizacjami lub osobami.
9. Dostępna musi być opcja załączenia elektronicznych dokumentów do wybranych pozycji w majątku lub licencji (faktury, dokumenty, itd.), preferowanie jest zapisywanie załączników w formie plików przed zapisywaniem ich w bazie danych.
10. Raporty w postaci list majątku, kart, specyfikacji, protokołów przeniesienia, usunięcia... powinny być łatwo dostępne i uruchamiać się bezpośrednio z głównego ekranu wyświetlającego majątek. Raporty dodawane lub modyfikowane przez administratora muszą być dostępne z tego samego menu.
11. System musi umożliwiać ewidencjonowanie działań takich jak np. wprowadzenie do użytkowania, naprawy, przesunięcia i wycofanie.
12. System musi posiadać opcje potwierdzenia przekazania majątku użytkownikowi za pomocą strony www.
13. System musi posiadać aplikację na urządzenia z systemem Android do sczytywania kodów kreskowych (zamiast terminali). Aplikacja po zeskanowaniu kodu kreskowego musi wyświetlać dane dotyczące zeskanowanego obiektu (nazwa, użytkownik, lokalizacja, nr ewidencyjny, ...). Aplikacja musi umożliwiać także wprowadzanie nowych pozycji majątku podczas inwentaryzacji, określenie dokładnego położenia majątku (piętro, pokój, użytkownik itp.), daty inwentaryzacji.
14. Aplikacja mobilna do sczytywania kodów kreskowych powinna umożliwiać bezpośrednią synchronizację z bazą danych. Aplikacja musi umożliwiać również tryb "offline", czyli do synchronizacji powinno dochodzić tylko wtedy, kiedy osoba inwentaryzująca zdecyduje o tym. Aplikacja musi umożliwiać przeprowadzenie całego procesu inwentaryzacji bez dostępu do sieci/bazy danych.
15. System musi posiadać opcję Inwentaryzacji za pomocą interface webowego. Każdy użytkownik musi zostać powiadomiony o konieczności wypowiedzenia się na temat posiadanego sprzętu. Po kliknięciu na link, ma mu się otworzyć strona, na której musi potwierdzić lub skorygować informacje o posiadanym sprzęcie.
16. Automatyczne tworzenia historii komputera – system musi umożliwiać stwierdzenie, kiedy np. doszło do zmiany użytkownika komputera bez aktywnego wprowadzenia informacji o przeniesieniu (automatyczne wykrywanie/rejestrowanie zmiany użytkownika).
17. Moduł do ewidencji majątku musi umożliwiać ewidencjonowanie akcesoriów do danego sprzętu. Akcesoria mają być pozycją, którą można bardzo szybko przypisać do danego obiektu i nie posiadają szczegółów (takich jak nr ewidencyjny, seryjny, …). Przykładem niech będzie np. etui i ładowarka przypisana do laptopa.
18. Powinna istnieć opcja oznaczania symbolem (np. gwiazdką) ulubionych pozycji w module majątku.
19. Musi istnieć opcja powielania majątku. Powielanie spowoduje skopiowanie cech wybranej pozycji takich jak typ, nazwa, lokalizacja, itd.

Zdalne zarządzanie

1. System musi posiadać opcję zdalnego zarządzania stacjami:
   1. przejęcie kontroli (przejęcie obecnej sesji użytkownika), przesyłanie wiadomości, sprawdzenie jakości połączenia, możliwość kopiowania plików, przejmowanie monitora, myszy, klawiatury; zdalne wyłączanie komputera, zdalny restart.
   2. skan otwartych i zamkniętych portów.
   3. skan stanu usług w momencie audytu.
   4. zdalne zarządzanie usługami (status, sposób uruchomienia).
   5. Remote Desktop Protocol – zdalny pulpit dostępny bezpośrednio z programu.
2. Powinien być dostępny zdalny pulpit również poza siecią lokalną - połączenie ma realizowane być za pomocą elementu pośredniczącego, który może być umieszczony w strefie zdemilitaryzowanej (DMZ) lub gdziekolwiek w Internecie, bez konieczności używania pośrednika trzecich stron.
3. System powinien umożliwiać pobranie przynajmniej podstawowych danych za pomocą protokołu SNMP - możliwość wyszukiwania drukarek, urządzeń sieciowych, NAS-ów i dodawania ich do modułu majątku.

Zdalna zbiorcze zarządzanie (skryptowanie, instalacje, ...)

1. System musi umożliwiać wykonywanie następujących czynności zbiorczo, bez interakcji użytkownika docelowego sprzętu: instalacja oprogramowania, odinstalowanie programu, kopiowanie plików na docelową stację, kasowanie plików i katalogów, uruchamianie skryptów lub plików wykonywalnych, wyłączenie i restart komputera, wylogowanie użytkownika (również poza siecią lokalną).
2. Musi istnieć opcja zdefiniowania kilku serwerów, z których będą przebiegały instalacje.
3. System musi umożliwiać warunkowe wykonywanie poszczególnych kroków zadań: bez poprawnego wykonania działania, następne działania nie zostaną uruchomione.
4. Musi istnieć opcja zaplanowania wykonania działań, niezależnie od tego, czy wybranego komputery za włączone lub wyłączone.

Alertowanie zdarzeń

1. System musi umożliwiać powiadamianie za pomocą maila oraz wyskakujących okien.
2. Musi istnieć opcja definiowania dni poprzedzających notyfikację związaną z zdarzeniem (np. miesiąc przed, tydzień przed, dzień przed i każdy dzień po terminie).
3. System musi oferować przynajmniej powiadomienia o wygasających licencjach i gwarancjach. Plusem jest możliwość definiowania własnych powiadomień.
4. System musi umożliwiać wysyłanie powiadomień związanych ze zbliżającym się terminem przeglądu, lub listą urządzeń, na których nie zostały wykonane czynności serwisowe w terminie.
5. Musi istnieć opcja wysyłania alertów/maila w przypadku usunięcia użytkownika z Active Directory z informacją o tym, że powinien oddać przypisany mu majątek IT.

Podstawowe wymagania modułu:

1. Monitoring i blokowanie aplikacji.
2. Monitoring i blokowanie stron www.
3. Monitoring i blokowanie dysków USB.
4. Monitoring wydruków.
5. Monitoring obciążenia komputerów.

Monitoring

1. System musi umożliwiać monitoring czasu pracy w aplikacji, ilość naciśnięć klawiszy klawiatury, ilość kliknięć myszką, podział czasu działania aplikacji na czas pracy (od momentu włączenia do momentu wyłączenia aplikacji) oraz czas aktywności (rzeczywisty czas aktywności użytkowników, okno (on top) na ekranie), statystyki wg czasu, grup, aplikacji.
2. Monitoring musi umożliwiać ustawienie czasu nieaktywności (timeout naliczania aktywności) - po określonym czasie nieaktywności, licznik czasu spędzonego pracą w aplikacji, zostanie zatrzymany.
3. Muszą być do dyspozycji informacje o odwiedzanych przez użytkowników stronach www: czas, statystyki wg domeny, czasu, użytkownika, konkretnych stron, czas pracy, czas aktywności użytkownika, dokładny adres strony www – aktywny odnośnik, tytuł strony.
4. Monitoring musi zbierać wartości obciążenia procesora i wykorzystania pamięci.
5. Monitoring musi umożliwiać (opcjonalne) śledzenie ruchu na kartach sieciowych komputera. Monitorowana ma być ilość pobranych (download) oraz wysłanych (upload) danych.
6. Agent musi umożliwiać monitoring wydruków (jakie dokumenty, ile, z jakiej drukarki, kiedy, jaki użytkownik drukował, wysokość i szerokość kartki, liczba kopii, kolor, wydruk obustronny).
7. System musi umożliwiać monitorowanie zmian na dyskach USB (zmiana nazwy pliku, wielkości, kasowanie pliku, itp.).
8. System musi umożliwiać monitorowanie zmian w wybranych katalogach (zmiana nazwy pliku, wielkości, kasowanie pliku, modyfikacja itp.).
9. Agent musi wspierać ustawienie przedziału czasowego monitoringu (np. od 7:00 do 15:00), wyłączenie monitorowania w weekendy.
10. Agent musi się automatycznie aktualizować do najnowszej wersji – można określić częstotliwość sprawdzania nowej wersji agentów lub konfiguracji. Równocześnie można określić częstotliwość wysyłania wyników monitoringu ze stacji.
11. Agent musi umożliwiać wysyłanie wyników monitoringu z dowolnego miejsca w internecie do centrali.
12. Agent musi umożliwiać wyłączenie poszczególnych dziedzin monitoringu: www, aplikacje, obciążenie procesora, obciążenie pamięci RAM, monitoring wydruków, czas zalogowania / wylogowania użytkownika.
13. System musi umożliwiać tworzenie dowolnej ilości profili monitoringu – można określić, w jakim zakresie będą poszczególne grupy komputerów monitorowane lub ograniczane.
14. Agent musi umożliwiać włączenie wyświetlania komunikatu przy starcie agenta. Tekst tego komunikatu musi być konfigurowalny w ustawieniach.

Agent musi umożliwiać blokowanie:

1. Blokowanie aplikacji – możliwość zdefiniowania aplikacji zabronionych i uniemożliwienie ich uruchomienia (także w przypadku kiedy użytkownik zmieni nazwę pliku uruchomieniowego). Musi istnieć opcja konfiguracji notyfikacji mailowej o tym zdarzeniu. Agent musi umożliwiać wyświetlenie informacji użytkownikowi o zablokowaniu aplikacji.
2. Blokowanie stron www, blokowanie wszystkich protokołów dla danej domeny, takich jak: http, https, ftp, imap, pop3, smtp, itp.
3. Blokowanie dysków USB wg numeru seryjnego dysku.
4. Autoryzacja dysków USB - definiowanie „białej listy” dysków USB i blokowanie nieautoryzowanych.
5. Blokowanie napędów CD/DVD.

Raportowanie

1. System musi oferować raporty z monitoringu (czasowe, wg użytkownika, wg kategorii, zbiorcze, szczegółowe …).
2. Tabele z wynikami monitoringu muszą umożliwiać sortowanie i filtrowanie wg jednostki organizacyjnej, lokalizacji, nazwy komputera, użytkownika....
3. System musi generować graficzne przedstawienie wyników – 3D wykresy (minimum 5 rodzajów) z legendą lub bez legendy.
4. System musi umożliwiać szybko zorientować się w negatywnych zjawiskach w organizacji za pośrednictwem raportów graficznych wyświetlających użytkowników (TOP 5 itp.), którzy korzystają z niepożądanych programów, gier, komunikatorów, multimediów, niepożądanych www, gier i rozrywki, portali społecznościowych, sklepów internetowych, użytkowników najwięcej drukujących dokumenty, wykonujących działania na USB, komputerów najbardziej obciążających CPU i RAM. Wszystko dla wybranego przedziału czasowego oraz (opcjonalnie) wybranego działu.
5. Mile widziana jest forma Dashboardu wyświetlającego dane monitoringu aktywności. Szybkie zestawienia dotyczące różnych aspektów zachowania użytkowników.
6. System musi oferować kategoryzację programów wg wykorzystania (np.: praca, zabawa, zabronione…) oraz wg typu programu (np.: gry, przeglądarki, antywirusy, …).
7. System musi umożliwiać kategoryzację stron www wg wykorzystania (zakazane, rozrywka, wiadomości i inne) oraz ich tematów (np. dla kobiet, sport, polityka, hazard, …).
8. System musi wyświetlać chronologicznie działania użytkownika w ciągu dnia od momentu zalogowania się aż po wylogowanie. Raport musi zawierać dane umożliwiające określenie, co użytkownik robił w danej chwili.
9. Musi istnieć opcja przeglądania wyników monitoringu przez www. Administrator musi mieć opcję ustawienia dostępu do raportów dla poszczególnych osób. Na przykład, manager działu produkcji ma dostęp do wyników swoich pracowników oraz działu przygotowania.

Podstawowe wymagania modułu:

1. Zarządzanie zgłoszeniami.
2. Historia zgłoszeń.
3. Kategorie i priorytety zgłoszeń.
4. Baza wiedzy, często zadawane pytania.
5. Integracja z e-mailem.

Ogólne

1. System musi umożliwiać integrację z Active Directory oraz autoryzację na poziomie AD. Dostępny również musi być Single sign-on (SSO).
2. Użytkownik musi mieć opcję zgłaszania problemu za pomocą maila z możliwością załączenia dowolnych załączników, które są zapisywane w HD.
3. Helpdesk musi być zintegrowany z oprogramowaniem audytującym – dane z audytu muszą być dostępne bezpośrednio z interface helpdesku.

Raporty

1. Raporty muszą być dostępne bezpośrednio w Helpdesku oraz (jeżeli system posiada) w aplikacji natywnej przeznaczonej do zarządzania systemem. Raporty muszą umożliwiać czasowe ograniczenie danych.
2. Helpdesk musi umożliwiać ewidencję kosztów oraz realnego czasu pracy na zgłoszeniu.
3. Użytkownik musi mieć możliwość na głównym ekranie obejrzenia wykresu stanu wszystkich jego zgłoszeń.
4. System musi oferować następujące rodzaje raportów:
   * statystyki zgłoszeń w poszczególnych kategoriach, dane pozwalające na ocenę pracy serwisantów,
   * statystyki zgłoszeń w danym przedziale czasowym wg kategorii, serwisanta, stanu,
   * zestawienia zawierające KPI, czyli indeks skuteczności realizacji zgłoszeń przez serwisantów,
   * raporty pozwalające na analizę wydajności serwisantów na podstawie SLA (czasu reakcji) w poszczególnych kategoriach zgłoszeń oraz na podstawie wyrabiania się w terminie oczekiwanego rozwiązania problemu,
   * zestawienia pozwalające na analizę kosztów związanych z realizacją zgłoszeń w danych kategoriach,
   * raporty realnego czasu spędzonego nad poszczególnymi zgłoszeniami.

Powiadomienia

1. System musi oferować możliwość dodatkowej komunikacji pomiędzy serwisantem a zgłaszającym (dopytanie zgłaszającego, odpowiedź zgłaszającego na pytanie).
2. Zdarzenia w helpdesku muszą generować powiadomienia mailowe do użytkownika oraz serwisanta – nowe zgłoszenie, zmiana stanu zgłoszenia i inne operacje ze zgłoszeniem.
3. System musi mieć opcję powiadamiania serwisantów/managerów o zalegających/nierozwiązanych zgłoszeniach.
4. **System musi umożliwiać dokładną konfigurację notyfikacji mailowej:**

- określenie treści maila w HTML,

- określenie tytułu maila,

- opcjonalne wysyłanie powiadomienia po zmianie stanu zgłoszenia, przypisaniu serwisanta, po wysłaniu wiadomości (chat),

- konfigurowalne wysyłanie powiadomienia przy zmianie stanu zgłoszenia - opcja włączenia/wyłączenia powiadomienia dla poszczególnych stanów i rodzajów użytkowników (użytkownik, serwisant, menadżer).

1. **Użytkownik musi mieć opcję odpowiedzi na pytanie serwisanta bezpośrednio za pomocą maila. Wiadomość użytkownika zostanie przypisana jako wiadomość do danego zgłoszenia.**
2. **Helpdesk musi umożliwiać komunikację ze wsparciem tylko za pomocą klienta pocztowego, bez konieczności logowania się do interfejsu webowego, wszelkie zdarzenia są jednak zapisywane w helpdesku.**
3. **System musi oferować opcję wyświetlania dowolnego tekstu po wyborze kategorii (kolejki). Tekst ten ma w dobrze widoczny sposób informować użytkownika o tym, na jakich zasadach powinien zgłaszać w danej kategorii. Na przykład można wyświetlać komunikat informujący o braku dostępu do poczty i przewidywanym czasie przywrócenia usługi, jeżeli użytkownik wybierze kategorię E-mail.**

Baza wiedzy

1. System musi posiadać bazę wiedzy – musi ona umożliwiać tworzenie treści na podstawie istniejących zgłoszeń.
2. System musi posiadać bazę wiedzy serwisantów – oddzielna baza wiedzy – tylko dla serwisantów.
3. Helpdesk dodatkowo musi posiadać moduł często zadawanych pytań (FAQ). Musi istnieć opcja fulltekstowego wyszukiwania. FAQ-u muszą umożliwiać tworzenie treści z palca lub na podstawie konwersji istniejącego zgłoszenia.

Obsługa systemu

1. Helpdesk musi posiadać różne poziomy uprawnień (użytkownik, serwisant, menadżer, administrator, ...)
2. Musi istnieć opcja załączania wielu elektronicznych załączników do zgłoszenia.
3. Musi istnieć opcja ustawienia dostępu do podglądu posiadanego majątku użytkownika.
4. Użytkownik musi mieć możliwość akceptacji lub ponownego otwarcia zgłoszenia.
5. Helpdesk musi umożliwiać dostosowanie szaty graficznej w postaci tematów graficznych oraz ukrycia elementów, podmiany logo na własne, itp.
6. Panel administracji zgłoszeń musi umożliwiać wykonywanie zbiorczych operacji na zgłoszeniach.
7. Helpdesk musi posiadać wielopoziomową kategoryzację zgłoszeń – liczba poziomów powinna być duża lub nieograniczona.
8. Helpdesk musi umożliwiać przypisywanie dowolnej liczby serwisantów do poszczególnych kategorii (kolejek) zgłoszeń.
9. Helpdesk musi umożliwiać ustawienie priorytetów (czasu rozwiązania) zgłoszeń niezależnie dla każdej kategorii. Priorytety powinny (opcjonalnie) determinować czas oczekiwanego rozwiązania.
10. System musi umożliwiać ustawienie sztywnego terminu dla każdej kategorii/kolejki (np. awarię drukarki rozwiązujemy do 8 godzin, bez możliwości wyboru).
11. **System musi umożliwiać zdefiniowanie czasu pracy serwisu w poszczególnych dniach (następnie** przypisania czasu pracy serwisu do poszczególnych kategorii/kolejek). Musi istnieć opcja zdefiniowania wielu serwisów pracujących w różnych czasach. Czas pracy serwisu musi mieć wpływ na obliczanie oczekiwanego terminu rozwiązania zgłoszenia.
12. Helpdesk musi posiadać tryb, w którym użytkownik może wybrać oczekiwaną datę oraz godzinę rozwiązania zgłoszenia.
13. Helpdesk musi umożliwiać tworzenie dowolnych formularzy do danej kategorii/kolejki zgłoszeń. Musi istnieć opcja posiadania specjalnych kategorii, w których temat i treść zgłoszenia są albo wypełnione automatycznie przez system, albo ukryte (taka kategoria służy do zebrania danych tylko za pomocą formularza). Pola formularza muszą posiadać opcję „Widoczny tylko dla serwisantów”.
14. Helpdesk musi umożliwiać formatowanie pól formularza. Dostępne muszą być wszystkie tagi HTML dla pytania (tekstu opisującego dane pole formularza).
15. Administrator musi mieć możliwość tworzenia jakiejś formy ogłoszeń. Te ogłoszenia muszą być widoczne na głównej stronie helpdesku. Ogłoszenia muszą umożliwiać dodawanie załączników oraz określenie dat od kiedy do kiedy mają się zgłoszenia wyświetlać.
16. Helpdesk musi posiadać jakiś system zatrzymania czasu zgłoszenia, jeżeli nastaną obiektywne okoliczności nieumożliwiające rozwiązanie w oczekiwanym terminie.
17. System musi wspierać protokół OAUTH2 podczas łączenia się z serwerem POP3/IMAP w celu zaciągnięcia zgłoszeń do HD.
18. **Helpdesk musi umożliwiać wyświetlanie tylko wybranych kategorii na podstawie lokalizacji użytkownika.** Na przykład: użytkownik z działu HR zobaczy inny zestaw kategorii niż użytkownik z działu informatyki.
19. System musi mieć opcję rozbicia zgłoszenia na zgłoszenia podrzędne (zadania tworzone w innych kategoriach/kolejkach).
20. Helpdesk musi umożliwiać zatwierdzanie zgłoszeń – system musi umożliwiać utworzenie kategorii/kolejek, w których wszystkie zgłoszenia muszą być zatwierdzone. Dodatkowo musi istnieć opcja wygenerowania prośby o zatwierdzenie przez serwisanta.
21. System musi posiadać system automatycznego rozbicia zgłoszenia na podrzędne zgłoszenia/zadania. Na przykład: wpada zgłoszenie dotyczące utworzenia nowej maszyny wirtualnej dla testów: system automatycznie (na podstawie predefiniowanych reguł) generuje zgłoszenia podrzędne do zarządzającego serwerami oraz do osoby zarządzającej środowiskiem testowym.
22. Każda kategoria/kolejka musi posiadać opcję konfiguracyjną wymuszającą zatwierdzenie zgłoszenia przez wszystkich przypisanych zatwierdzających oraz ustawienie, które mówi, że wystarczy by jeden zatwierdzający się zgodził.
23. Podczas wypełniania formularza zgłoszenia, system musi podpowiadać potencjalne rozwiązania, bazując na temacie zgłoszenia.
24. Administrator musi mieć opcję ustawienia wybranych kategorii/kolejek tak, by wszystkie zgłoszenia w nich wymagały od serwisantów podania kosztów/realnego czasu pracy nad zgłoszeniem.
25. System musi uwzględniać dni wolne od pracy podczas obliczania terminu oczekiwanego rozwiązania. Helpdesk musi posiadać opcję definiowania dni wolnych od pracy. Mile widziana jest opcja definicji świąt powtarzających się co roku.

## System do zbierania i analizy logów

Parametry techniczne minimum:

Wymagania funkcjonalne

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 mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
7. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20  GB danych dziennie
8. System musi zapewniać retencję danych w okresie minimum 365  dni.
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
14. 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 .
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
18. Interfejs musi posiadać angielską lub polską wersję językową.
19. 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).
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
23. System musi wspierać mechanizm logowania typu Single Sign On.
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
26. 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.
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
31. System musi pozwalać na tworzenie parserów z poziomu GUI
32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
37. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

* Syslog,
* WEF,
* Flat file,
* Event log,
* WMI,
* SNMP trap,
* XML,
* JSON,
* JDBC/ODBC
* CSV,
* Email,

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

1. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
2. 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.
3. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
4. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
5. 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.
6. System musi posiadać predefiniowany zestaw parserów zdarzeń.
7. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
8. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
9. 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.
10. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
11. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
12. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
13. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
14. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
15. 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.
16. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
17. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
18. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
19. Wykrycia dowolnej treści w logach,
20. Wykrycia wystąpienia wartości pola na wybranej liście,
21. Wykrycia niewystępowania wartości pola na wybranej liście,
22. Wykrycia zmiany jednego z kilku pól,
23. Wykrycia zdarzeń występujących z zadaną częstotliwością,
24. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
25. Wykrycia zaniku Wiadomości,
26. Wykrycia nowej wartości pola w zadanym okresie czasu,
27. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
28. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
29. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
30. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
31. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
32. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
33. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
34. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
35. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
36. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
37. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
38. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
39. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
40. 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.
41. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
42. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
43. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
44. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
45. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
46. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres minimum 12 miesięcy.
47. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
48. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
49. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
50. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
51. System musi umożliwiać integrację z Mitre ATT@CK.

Reguły korelacyjne, alerty i obsługa incydentów

1. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
2. 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.
3. 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.
4. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
5. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit’u i wykrywania ukrytych procesów, plików, portów
6. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
7. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

Szkolenia

1. Wykonawca dostarczy voucher szkoleniowy dla 2-óch słuchaczy zarówno dla systemu SIEM.
2. Szkolenie odbędzie się w formie zdalnej.
3. Szkolenie musi być prowadzone w języku polskim.
4. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
5. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.

Wdrożenie

1. Opracowanie harmonogramu wdrożenia systemu SIEM.
2. Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia.
3. Przeprowadzenie instalacji i konfiguracji systemu SIEM.
4. Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych.
5. Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.
6. Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.
7. Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.
8. Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.

* Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.

## Szkolenia produktowe dla administratora z dostarczonego sprzętu teleinformatycznego

#### Szkolenie wraz z wdrożeniem oferowanego systemu Firewall (UTM)

Opis ogólny:

Szkolenie techniczne poświęcone urządzeniom do ochrony styku sieci firmowej z Internetem.

Od Wykonawcy oczekuje się wdrożenia oprogramowania wraz z pełną konfiguracjąiI integracją z infrastrukturą informatyczną Zamawiającego.

Minimalny zakres szkolenia:

1. Rozpoczęcie pracy z urządzeniem
   * Rejestracja w strefie klienta i dostęp zasobów
   * Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
   * Ustawienia systemowe i uprawnienia administratorów
   * Instalacja licencji i aktualizacja systemu
   * Tworzenie kopii zapasowej i przywracanie konfiguracji
2. Zbieranie logów i monitorowanie
   * Przedstawienie kategorii zbieranych logów
   * Wykresy historyczne i monitorowanie
3. Obiekty
   * Typy obiektów oraz ich wykorzystanie
   * Obiekty sieciowe i obiekt typu „router”
4. Konfiguracja sieci
   * Tryby pracy urządzenia
   * Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
   * Typy routingu oraz ich priorytety
5. Translacja adresów sieciowych (NAT)
6. Translacja połączeń wychodzących (maskarada)
7. Translacja połączeń przychodzących (przekierowanie)
8. Translacja dwukierunkowa (jeden do jeden)
9. Filtrowanie ruchu sieciowego (Firewall)
10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
    * Szczegółowy opis parametrów reguły Firewall
    * Kolejność przetwarzania reguł Firewall i NAT
11. Ochrona aplikacji
    * Implementacja filtrowania URL dla ruchu http i https
    * Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
    * Moduł IPS i stosowanie profili inspekcji
12. Użytkownicy i uwierzytelnianie
13. Konfiguracja usługi katalogowej
    * Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
    * Rejestracja użytkowników
    * Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
14. Wirtualne sieci prywatne (VPN)
    * Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
    * Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
    * Tunele VTI
15. SSL VPN
    * Zasada działania
    * Konfiguracja

#### Szkolenie z Administracji i zarządzania systemami pamięci masowej

**Opis ogólny:**

To zaawansowane szkolenie jest skierowane do administratorów IT oraz specjalistów zajmujących się zarządzaniem systemami backupu i NAS (Network Attached Storage) w organizacjach. Uczestnicy zdobędą kompleksową wiedzę na temat instalacji, konfiguracji oraz zaawansowanych funkcji oferowanych przez oprogramowanie do backupu i systemy NAS. Program obejmuje szeroki zakres tematów, w tym:

Wprowadzenie:

•        Wprowadzenie do szkolenia, cele i oczekiwania.

•        Przegląd agendy i struktury szkolenia.

•        Omówienie korzyści z zastosowania systemów NAS w przedsiębiorstwie.

Przegląd Produktów NAS:

•        Omówienie różnych modeli systemów NAS i ich zastosowań.

•        Podstawowe funkcje i możliwości sprzętowe i programowe.

•        Przykłady wdrożeń systemów NAS w różnych branżach.

Podstawowe Informacje o Możliwościach Sprzętowych i Programowych:

•        Szczegółowy przegląd architektury sprzętowej.

•        Wprowadzenie do oprogramowania systemowego i jego funkcji.

•        Zarządzanie zasobami sprzętowymi i programowymi w systemach NAS.

Zarządzanie Dyskami i Konfiguracja Przestrzeni:

•        Podstawy zarządzania dyskami w systemach NAS.

•        Procedury instalacji i konfiguracji dysków twardych.

•        Monitorowanie stanu dysków i rozwiązywanie problemów.

Architektura Przestrzeni Dyskowej:

•        Szczegółowe omówienie architektury pamięci masowej w systemach NAS.

•        Koncepcje i komponenty systemów przechowywania danych.

•        Zarządzanie przestrzenią dyskową i optymalizacja wydajności.

Dobór Dysków Twardych i Możliwości Konfiguracji:

•        Kryteria doboru dysków twardych do systemów NAS.

•        Przegląd różnych typów dysków (HDD, SSD) i ich zastosowań.

•        Konfiguracja RAID i innych technologii ochrony danych.

Konfiguracja Woluminów:

•        Tworzenie i zarządzanie woluminami na urządzeniach NAS.

•        Optymalizacja przestrzeni dyskowej i zarządzanie zasobami.

•        Monitorowanie i rozszerzanie woluminów.

Konfiguracja iSCSI LUN:

•        Tworzenie i zarządzanie jednostkami logicznymi (LUN).

•        Integracja systemów NAS z serwerami i innymi urządzeniami.

•        Zarządzanie dostępem iSCSI LUN.

Konfiguracja SSD Cache:

•        Implementacja i zarządzanie pamięcią cache SSD.

•        Optymalizacja wydajności systemu poprzez przyspieszenie operacji odczytu/zapisu.

•        Monitorowanie i zarządzanie zasobami cache.

Chmura:

•        Integracja z usługami chmurowymi i zdalnymi zasobami.

•        Zarządzanie danymi w chmurze i synchronizacja z lokalnymi zasobami.

Przechowywanie Danych:

•        Metody i strategie przechowywania danych.

•        Zarządzanie przestrzenią dyskową i optymalizacja jej wykorzystania.

•        Wdrażanie polityk przechowywania i archiwizacji danych.

Zarządzanie Uprawnieniami:

•        Konfiguracja uprawnień użytkowników i grup.

•        Zarządzanie dostępem do zasobów i monitorowanie aktywności.

•        Implementacja polityk bezpieczeństwa dostępu.

Udziały Sieciowe:

•        Tworzenie i zarządzanie udziałami sieciowymi.

•        Konfiguracja dostępu i uprawnień do udziałów sieciowych.

•        Monitorowanie i zarządzanie udostępnionymi zasobami.

Backup i Replikacja:

•        Strategie backupu i replikacji danych.

•        Konfiguracja i zarządzanie kopiami zapasowymi.

•        Wdrażanie polityk backupu i odzyskiwania danych.

Narzędzie do Backup’u i Synchronizacji:

•        Wprowadzenie do narzędzia backupu i synchronizacji.

•        Konfiguracja i zarządzanie synchronizacją i backupem danych.

Deduplikacja:

•        Techniki deduplikacji danych.

•        Konfiguracja i zarządzanie deduplikacją.

•        Optymalizacja przestrzeni dyskowej poprzez deduplikację.

Wirtualizacja:

•        Podstawy wirtualizacji na systemach NAS.

•        Tworzenie i zarządzanie maszynami wirtualnymi.

•        Integracja wirtualizacji z innymi zasobami IT.

Wirtualizacja na NAS:

•        Implementacja rozwiązań wirtualizacyjnych na systemach NAS.

•        Zarządzanie zasobami wirtualnymi.

•        Monitorowanie wydajności i rozwiązywanie problemów.

Kontenery:

•        Wprowadzenie do technologii kontenerów.

•        Tworzenie i zarządzanie kontenerami na systemach NAS.

•        Integracja kontenerów z innymi zasobami i usługami.

Zabezpieczenie Systemów NAS:

•             Metody zabezpieczania systemów NAS.

•             Implementacja polityk bezpieczeństwa i zarządzanie ryzykiem.

•             Monitorowanie i reagowanie na zagrożenia.

Narzędzie do Analizy Bezpieczeństwa:

•             Wprowadzenie do narzędzia analizy bezpieczeństwa.

•             Konfiguracja i zarządzanie bezpieczeństwem systemu.

•             Wdrażanie rekomendacji i polityk bezpieczeństwa.

Zabezpieczenie przed Atakami Brute Force:

•             Metody ochrony przed atakami brute force.

•             Konfiguracja zabezpieczeń i polityk dostępu.

•             Monitorowanie i reagowanie na próby ataków.

Konfiguracja Antywirusa:

•             Implementacja i zarządzanie oprogramowaniem antywirusowym.

•             Skanowanie i ochrona systemu przed zagrożeniami.

•             Automatyzacja procesów skanowania i aktualizacji.

Szyfrowanie Dysków i Katalogów:

•        Techniki szyfrowania danych.

•        Konfiguracja szyfrowania na poziomie dysków i katalogów.

•        Zarządzanie kluczami szyfrowania i politykami dostępu.

Zarządzanie Hasłami Użytkowników:

•        Polityki zarządzania hasłami.

•        Implementacja i zarządzanie politykami bezpieczeństwa haseł.

•        Monitorowanie i audytowanie zmian haseł i dostępu.

#### Szkolenie z zakresu oferowanego i wdrożonego przez Wykonawcę oprogramowania do backup

Opis i zakres szkolenia:

Moduł 1. Wstep

* Wprowadzenie do tematyki szkolenia

Moduł 2. Przegląd portfolio,

* Produkty i pakiety

Moduł 3. Architektura

* Kluczowe komponenty systemu i ich współpraca
* Komponenty opcjonalne
* Scenariusze implementacji
* Warunki wstępne
* Rozbudowa

Moduł 4. Wstępna konfiguracja

* Dodawanie serwerów
* Konfiguracja polityk kopii i odtworzenia
* Zarządzanie ruchem sieciowym
* Ustawienia powiadomień globalnych
* Interfejs użytkownika

Moduł 5. Ochrona

* Tworzenie zadań backupowych
* Tworzenie punków odtworzenia z użyciem produktu
* Kopiowanie
* Replikacja

Moduł 6. Odtworzenie maszyny wirtualnej

* Odtworzenie maszyny wirtualnej
* Praca z produktem
* Wgląd w odtworzenie z repliki (Recovery from Replica)

Moduł 7. Odtworzenie pojedynczego obiektu

* Odtworzenie na poziomie pojedynczego obiektu (pliku)

Moduł 8. Zaawansowana ochrona danych

* Współpraca z rozwiązaniami taśmowymi
* Wsparcie dla systemów pamięci masowych
* Współpraca z repozytoriami z deduplikacją
* Zastosowanie

Moduł 9. Funkcje i możliwości

* Automatyczne wykrywanie infrastruktury kopii zapasowych i wirtualnej
* Kategoryzacja
* Uprzednio zdefiniowane alerty
* Zautomatyzowany monitoring
* Raportowanie i pulpity
* Bezagentowe gromadzenie danych
* Specyficzne funkcje dla Hyper-V
* Wdrażanie
* Narzędznia oceny

Moduł 10. Wersje systemu

* Omówienie i porównanie wersji produktu
* Pełne oraz bezpłatne moduły

Moduł 11. Rozwiązywanie problemów

* Identyfikacja problemu
* Przegląd i analiza problemu
* Poszukiwanie dodatkowych informacji
* Pomoc techniczna producenta

#### Szkolenie z zakresu oferowanego i wdrożonego przez Wykonawcę oprogramowania do zarzadzania sieci

Opis i zakres szkolenia:

* **Jak wykonać wewnętrzny audyt legalności oprogramowania – SAM**
* **Jak rozpocząć zbieranie danych o infrastrukturze IT**
* **Jak wprowadzać i rozliczać licencje na oprogramowanie.**
* **Jak zarządzać kodami kreskowymi i wykonać inwentaryzację majątku**
* **Jak włączyć powiadomienia o zdarzeniach w sieci oraz wygasających terminach**
* **Jak zbiorczo i automatycznie instalować oprogramowanie na stacjach.**
* **Dzielenie się wiedzą i praktyką z zakresu wykorzystania systemu w różnych aspektach pracy**
* **Jak analizować zachowania użytkowników w kontekście cyberbezpieczeństwa, a tym samym podnosić poziom ochrony organizacji.**
* **Jak ograniczyć dostęp do serwisów społecznościowych oraz zmniejszyć ryzyko wycieku danych**
* **Jak zaimplementować system zgłoszeń w organizacji**
* **Jak usprawnić komunikację oraz realizację zadań**
* **Jak sprostać wymogom dyrektywy unijnej dotyczącej zgłoszeń anonimowych**
* **Nowości w systemie, indywidualne konsultacje, rozdanie certyfikatów.**

#### Szkolenie z Administracji Active Directory na Microsoft Windows Server

#### Opis Szkolenia:

#### To intensywne szkolenie jest przeznaczone dla administratorów systemów oraz specjalistów IT, którzy chcą zdobyć zaawansowaną wiedzę i umiejętności w zakresie instalacji, konfiguracji i zarządzania usługą Active Directory na platformie Microsoft Windows Server. Uczestnicy nauczą się nie tylko podstawowych operacji, ale także zaawansowanych technik zabezpieczania i optymalizacji środowiska Active Directory. Program obejmuje także dodatkowe moduły dotyczące integracji z serwerami certyfikatów oraz Network Policy Server (RADIUS).

Plan Szkolenia:

1. Instalacja Active Directory na Microsoft Windows Server:

* Przygotowanie serwera do instalacji roli Active Directory.
* Konfiguracja pierwszego kontrolera domeny.
* Procedura instalacji usług AD DS.

2. Podstawowe narzędzia do zarządzania Active Directory:

* Przegląd narzędzi zarządzania, takich jak Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts.

3. Zarządzanie użytkownikami:

* Dodawanie nowych użytkowników do domeny.
* Konfiguracja właściwości obiektów użytkowników.
* Zarządzanie grupami użytkowników.
* Przyznawanie i zarządzanie uprawnieniami użytkowników.

4. Rola DNS w Active Directory:

* Integracja usługi DNS z Active Directory.
* Konfiguracja stref DNS i rekordów SRV.

5. Dodawanie komputerów do Active Directory:

* Procedura dołączania komputerów do domeny.
* Konfiguracja zabezpieczeń komputerów w kontekście domeny.

6. Polityki grup:

* Stosowanie polityk grup do zabezpieczania i zarządzania środowiskiem Active Directory.
* Przekierowanie folderów użytkowników na serwerze plików przy użyciu polityk grup.
* Instalacja oprogramowania przy pomocy GPO (Group Policy Objects).

7. Dodawanie kolejnych kontrolerów do domeny Active Directory - redundancja:

* Procedura dodawania dodatkowych kontrolerów domeny.
* Przenoszenie ról FSMO (Flexible Single Master Operation) pomiędzy kontrolerami.

8. Windows Server Backup:

* Konfiguracja i zarządzanie kopiami zapasowymi systemu Active Directory.
* Przywracanie danych z kopii zapasowych.

9. Firewall w systemie Windows Server:

* Dodawanie i edycja reguł firewalla systemowego Windows Server.
* Konfiguracja zabezpieczeń sieciowych na poziomie serwera.

10. Network Policy Server (RADIUS) i jego integracja z Active Directory:

* Konfiguracja Network Policy Server do autoryzacji i uwierzytelniania sieciowego.
* Integracja NPS z usługą Active Directory.

11. Usługi Active Directory Certificate Services:

* Przegląd usług AD CS i ich zastosowań.
* Procedura instalacji i konfiguracji usług PKI w środowisku Active Directory

Sposób przeprowadzenia szkolenia:

Wykonawca przeprowadzi szkolenie dla administratora w trybie on-line

Szkolenie zostanie przeprowadzone przez Wykonawcę do 3 dni od dnia dostarczenia sprzętu do miejsca wskazanego przez Zamawiającego.