**ZAŁĄCZNIK NR 1**

|  |
| --- |
|  |
| Opis Przedmiotu Zamówienia |
| Oprogramowanie oraz infrastruktura sprzętowa  |

|  |
| --- |
|  |

Spis treści

[Wstęp 3](#_Toc176358537)

[I. Obszar techniczny 4](#_Toc176358538)

[1. UTM Unified Threat Management 4](#_Toc176358539)

[2. NAC Network Access Control 10](#_Toc176358540)

[3. Serwer typ 1 (serwery do klastra) 13](#_Toc176358541)

[4. Serwer typ 2 (serwer do zbierania logów) 22](#_Toc176358542)

[5. Serwer typ 3 (rozbudowa serwera AD) 31](#_Toc176358543)

[6. Macierz do klastra 34](#_Toc176358544)

[7. UPS do serwerowni 41](#_Toc176358545)

[8. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 42](#_Toc176358546)

[9. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 44](#_Toc176358547)

[10. Oprogramowanie do wykonywania kopii zapasowych 44](#_Toc176358548)

[11. Oprogramowanie SIEM Security Information and Event Management 48](#_Toc176358549)

[12. Oprogramowanie do monitorowania infrastruktury informatycznej 69](#_Toc176358550)

[II. Obszar kompetencyjny 75](#_Toc176358551)

[1. Szkolenia typ 1 (Szkolenia dla pracowników z działu IT) 75](#_Toc176358552)

# Wstęp

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Miejskiej Pruszcz Gdański realizowanego w ramach „Cyberbezpieczny Samorząd” dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.

# Obszar techniczny

## UTM Unified Threat Management

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UTM Unified Threat Management (przedłużenie licencji posiadanego urządzenia UTM) |
| **Typ** | W ramach dostawy Zamawiający wymaga odnowienia serwisów i licencji dla posiadanego urządzenia FORTIGATE-300E o numerze seryjnym FG3H0E5819906114w zakresie minimum: * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
* Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

System musi być objęty serwisem producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach przedłużenia tych serwisów producent musi zapewnić dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Licencje i serwisy mają obowiązywać do 17.06.2026 r.Zamawiający dopuszcza dostarczenie urządzania klasy UTM równoważnego (tj. wymianę w/w urządzenia klasy UTM) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy rozwiązania równoważnego Zamawiający wymaga dodatkowo: - wdrożenia i montażu we wskazanej szafie RACK w siedzibie Zamawiającego- skonfigurowania dla wszystkich użytkowników - przeszkolenia administratorów z dostarczonego rozwiązania, wg ustaleń z Zamawiającym. |
| **OPIS RÓWNOWAŻNOŚCI – wymagania minimalne:** |
| **Wymagania ogólne** | System bezpieczeństwa realizujący wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.Mimalne parametry wydajnościowe:1. W zakresie Firewall’a obsługa nie mniej niż 4 mln. jednoczesnych połączeń oraz 300 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 30 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.8 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 18 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.8 Gbps

System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

Funkcje Systemu Bezpieczeństwa:W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

Połączenia VPN1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WANW zakresie routingu rozwiązanie zapewnia obsługę:1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.

Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP |
| **Ilość** | 1. szt.
 |

## NAC Network Access Control

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | NAC Network Access Control |
| **Wymagania minimalne** | W ramach dostawy Zamawiający wymaga dostarczenia systemu typu NAC zapewniającego kontrolę dostępu do sieci. Licencja bezterminowa, obowiązująca do 17.06.2026 r., obejmujące minimum 250 końcówek (MAC adres) jednocześnie łączących się z siecią |
| **Wymagania ogólne** | Główna funkcjonalność systemu w zakresie minimum: * Autoryzacja użytkowników i punktów końcowych w sieciach LAN, WiFi i VPN.
* Praca w sieciach heterogenicznych z urządzeniami sieciowymi, które spełniają standardy.
* Możliwość zarządzania i wizualizacji adresacji IP (funkcjonalność IPAM).
* Wbudowana funkcjonalność serwera DHCP.
* Wykrywanie obcych serwerów DHCP.
* Wsparcie dla protokołu Ipv6
* Monitorowanie SNMP urządzeń sieciowych z opcją bieżącego sprawdzania obciążenia, liczby uprawnień lub prawidłowej pracy urządzenia.
* Monitorowanie urządzeń końcowych za pomocą SNMP.
* Funkcjonalność zdalnej konfiguracji przełącznika na poziomie portu.
* Lokalna wbudowana baza danych z informacjami o użytkownikach i urządzeniach końcowych.
* Możliwość uwierzytelniania w oparciu o zewnętrzne bazy danych w tym AD, LDAP, SQL, Radius, G Suite, Facebook, Google.
* Praca w środowiskach z wieloma domenami (całkowicie niezależne domeny).
* Zarządzanie serwerami DNS.
* Wbudowany serwer RADIUS do obsługi autoryzacji w oparciu o protokół 802.1x.
* Obsługa różnych metod autoryzacji: 802.1X, na podstawie adresu MAC, za pośrednictwem Captive Portal.
* Możliwość resetowania haseł użytkowników domenowych przez Captive Portal lub Portal Zarządzający.
* Funkcja rozłączania oparta o protokół: RADIUS CoA, SNMP, Telnet / SSH.
* Rozbudowana funkcjonalność monitorowania i raportowania.
* Przebudowany i uproszczony panel Dashboard.
* Wbudowany serwer CA do obsługi autoryzacji przy użyciu własnych certyfikatów.
* Możliwość wdrożenia w środowiskach obsługiwanych przez wiele urzędów certyfikacji CA.
* Dystrybucji certyfikatów z zewnętrznych CA przez SCEP.
* Wbudowany serwer TFTP do użytku w dowolnym celu.
* W celu zapewnienia niezawodności działania w ramach podstawowej licencji systemu dostępna jest funkcjonalność HA.
* Wersja rozproszona dostępna w podstawowej wersji oprogramowania.
* Możliwość profilowania urządzeń końcowych.
* Funkcjonalność MUD (Manufacturer Usage Description).
* Dedykowany agent do kontroli poziomu bezpieczeństwa na urządzeniach końcowych.
* Rozłączanie sesji z wykorzystaniem agenta.
* Zaawansowany mechanizm detekcji NAT.
* One Time password authentication – dodatkowe zabezpieczenie przy logowaniu do sieci VPN (obsługa SMS/ tokenów).
* Automatyzacji procesów.
* Możliwość zarządzenia urządzeniami końcowymi przez Capitve Portal.
* Automatyczna konfiguracja sieci na urządzeniu końcowym.
* Możliwość tworzenia graficznych diagramów fizycznej topologii sieci.
* System musi posiadać interfejs w języku polskim
* Pomoc techniczna musi być świadczona w języku polskim

Wspierane przez system bazy przechowujące informację o użytkownikach i urządzeniach, minimum: * Lokalna wbudowana
* Microsoft Active Directory
* RADIUS (np. EDUROAM)
* LDAP
* Microsoft SQL, MySQL, PostgreSQL, Oracle, ODBC
* Kerberos
* przez API
* media społecznościowe
* G Suite

Obsługiwane metody autoryzacji, minimum: * PAP
* EAP-MD5
* CHAP, MSCHAPv1, MSCHAPv2
* EAP-TLS
* EAP-FAST (EAP-MSCHAPv2, EAP-TLS)
* PEAP (EAP-MSCHAPv2, EAP-TLS, EAP-PEAP)
* TTLS (EAP-MSCHAPv2, EAP-TLS, EAP-MD5)
* MAC
* Captive Portal (wbudowany, zewnętrzny na punkcie dostępowym, integracja z sieciami społecznościowymi,
* obsługa sponsorów)
* Kerberos
* Tacacs+

 Metody profilowania, minimum : * WMI
* SNMP
* NMAP
* TCP
* DHCP Fingerprinting
* DHCP SPAN
* Vendor OUI
* dedykowany Agent
* Active Directory
* HTTP/S
* CDP/LLDP
* MDM
* UTM
* NGFW
* DNS
* RADIUS
* API

 Dwukierunkowa komunikacja z systemami zewnętrznymi, minimum:* NGFW
* UTM
* IPS
* MDM
* Antywirus
* SIEM
* urządzenia sieciowe
* monitory ruchu sieciowego
 |
| **Wymagania dodatkowe** | Zamawiający w ramach dostawy wymaga także wdrożenia w zakresie minimum: Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku wirtualizacyjnym Zamawiającego.Podstawowa konfiguracja systemu (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).Integracja dostarczanych urządzeń sieciowych (switche, AP) z wdrażanym systemem, w ramach funkcjonalności dostępnych na urządzeniach. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.Uruchomienie uwierzytelniania w oparciu o adres MAC na wdrażanym systemie, testy.Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania wdrażanym systemem Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń. |
| **Ilość** | 1. szt.
 |

## Serwer typ 1 (serwery do klastra)

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Serwer typ 1 (serwery do klastra) |
| **Obudowa** | * Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji minimum 8 dysków 2.5”
* Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
* Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
 |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów.
* Obsługa procesorów minimum 32 rdzeniowych.
* Płyta główna musi być zaprojektowana przez producenta serwera
* Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
* Płyta główna powinna obsługiwać do 1TB pamięci RAM.
 |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
 |
| **Procesor** | * Zainstalowane minimum dwa procesory minimum 12-rdzeniowe, minimum 2.0GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku minimum 315 w teście SPECrate2017\_int\_base, dostępn ym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Wynik testu dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
 |
| **RAM** | * Minimum 256GB DDR5 RDIMM 4800MT/s,
 |
| **Funkcjonalność pamięci RAM** | * Demand Scrubing,
* Patrol Scrubing,
* Permanent Fault Detection
 |
| **Gniazda PCI** | * minimum trzy sloty PCIe
 |
| **Interfejsy sieciowe/SAS** | * Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz minimum 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
* Minimum Czteroportowa karta 10Gb Ethernet BaseT
* Minimum Czteroportowa karta 12Gb SAS HBA
 |
| **Dyski twarde** | Zainstalowane * Minimum 2x dysk SSD SATA o pojemności minimum 480GB, 6Gb, 2,5“ Hot-Plug.
* Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności minimum 960GB z możliwością konfiguracji RAID 1.
 |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
 |
| **Wbudowane porty** | * Minimum 4 x USB z czego nie mniej niż 1x USB 3.0, oraz minimum 2x VGA
 |
| **Kable/wkładki** | * Zainstalowane minimum dwie wkładki SFP+ SR 10Gbs 850nm LC DDM MMF 300m
 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
 |
| **Zasilacze** | * Redundantne, Hot-Plug minimum 1100W klasy Titanium
 |
| **System operacyjny/dodatkowe oprogramowanie** | Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie wszystkie core oferowanych procesorów. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym nielimitowanej ilości wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
* Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
 |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
* Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
 |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* + - zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
		- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
		- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
		- możliwość podmontowania zdalnych wirtualnych napędów;
		- wirtualną konsolę z dostępem do myszy, klawiatury;
		- wsparcie dla IPv6;
		- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
		- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
		- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
		- integracja z Active Directory;
		- możliwość obsługi przez dwóch administratorów jednocześnie;
		- wsparcie dla dynamic DNS;
		- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
		- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
		- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o:
		- Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
		- Przesyłanie danych telemetrycznych w czasie rzeczywistym
		- Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
		- Automatyczna rejestracja certyfikatów (ACE)
 |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:* + - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
		- integracja z Active Directory
		- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
		- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
		- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
		- Szczegółowy opis wykrytych systemów oraz ich komponentów
		- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
		- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
		- Grupowanie urządzeń w oparciu o kryteria użytkownika
		- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
		- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
		- Szybki podgląd stanu środowiska
		- Podsumowanie stanu dla każdego urządzenia
		- Szczegółowy status urządzenia/elementu/komponentu
		- Generowanie alertów przy zmianie stanu urządzenia.
		- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
		- Integracja z service desk producenta dostarczonej platformy sprzętowej
		- Możliwość przejęcia zdalnego pulpitu
		- Możliwość podmontowania wirtualnego napędu
		- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
		- Możliwość importu plików MIB
		- Przesyłanie alertów „as-is” do innych konsol firm trzecich
		- Możliwość definiowania ról administratorów
		- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
		- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
		- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
		- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
		- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
		- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
		- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
		- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
		- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
		- Zdalne uruchamianie diagnostyki serwera.
		- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
		- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
 |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:Monitoring:* ilość podłączonych oraz rozłączonych systemów
* stan podłączonych urządzeń
* informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
* Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
* informacje o statusie gwarancji dla poszczególnych urządzeń
* informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
* informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
* Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
* Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
* Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
* Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
* Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
* Monitoring parametrów serwerów z informacją o minimum:
* Obciążeniu procesora
* Zużyciu pamięci RAM
* Temperaturze procesorów
* Temperaturze powietrza wlotowego
* Zużyciu prądu
* Zmianach w fizycznej konfiguracji serwera
* Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
* Monitoring parametrów pamięci masowych z informacją o minimum:
* Opóźnieniach
* IOPS
* Przepustowości
* Utylizacji kontrolerów
* Pojemność całkowita i dostępna
* Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
* Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
* Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
* Informacje o poziomie redukcji danych
* Informacje o statusie replikacji oraz snapshotów
* Monitoring parametrów przełączników sieciowych z informacją o minimum:
* Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
* Stanie komponentów: zasilacze, wentylatory
* Podłączonych hostach
* Ilości i statusu portów
* Utylizacji procesora
* Utylizacji poszczególnych portów
* Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

Aktualizacja firmware* możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
* Raporty
* Możliwość generowania raportów dla serwerów zawierających informację o:
* Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
* Średnim obciążeniu: procesorów, pamięci RAM, IO,
* Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
* Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
* Generowanie raportów do plików CSV i PDF

Cyberbezpieczeństwo* Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
* Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
* Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
* Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.

Wspierane urządzenia* Urządzenie Producenta dostarczane w ramach postępowania
* Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)

Wirtualny asystent* Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;

Możliwość rozszerzenia funkcjonalności* Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.

Inne* Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

CertyfikatyOferowana platforma musi być zaprojektowana zgodnie ze standardami:* ISO 27001
* NIST Security and Privacy Controls for Federal Information Systems and Organization
* CSA Cloud Control Matrix
 |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub normami równoważnymi,
* Serwer musi posiadać deklaracja CE lub równoważną
* Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku (wydruk należy załączyć do oferty).
 |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
* Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
 |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 miesięcy.
* Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
* Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)
* Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
* Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
* Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
* Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
* Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
* Zamawiający wymaga dołączenia do oferty oświadczenia od producenta sprzętu lub autoryzowanego Partnera Serwisowego Producenta , że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
* Serwis urządzeń musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
* Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

Zamawiający wymaga dołączenia do oferty oświadczenia od producenta sprzętu potwierdzające, że serwis oferowanego serwera będzie: - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; - firma serwisująca posiada autoryzacje producenta oferowanego serwera; - firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. |
| **Wymagania dodatkowe** | Zamawiający w ramach dostawy wymaga dodatkowo wdrożenia w zakresie minimum:* wstępna konfiguracja karty zarządzającej ,
* aktualizacja firmware,
* wstępna konfiguracja systemu operacyjnego,
* montaż fizyczny u Zamawiającego,
* adresacja IP zgodnie z uzgodnieniami z Zamawiającym,
* podłączenie hostów do domeny Zamawiającego,
* podłączenie zasobów macierzy,
* wdrożenie usług -wirtualizacji,
* konfiguracja klastra wysokiej dostępności,
* przygotowanie testowej VM, testy migracji i redundancji zasilania i połączeń z macierzą,
* przygotowanie dokumentacji powdrożeniowej.
 |
| **Ilość** | 2 szt.  |

## Serwer typ 2 (serwer do zbierania logów)

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Serwer typ 2 (serwer do zbierania logów) |
| **Obudowa** | * Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug
* Obudowa z możliwością wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
* Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
 |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów.
* Płyta główna musi być zaprojektowana przez producenta serwera
* Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci
* Płyta główna powinna obsługiwać do 1TB pamięci RAM.
 |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
 |
| **Procesor** | * Zainstalowany minimum jeden procesor 16-rdzeniowy, minimum 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku minimum 231 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
 |
| **RAM** | * Minimum 64GB DDR4 RDIMM 3200MT/s,
 |
| **Funkcjonalność pamięci RAM** | * Advanced ECC,
* Memory Page Retire,
* Fault Resilient Memory,
* Memory Self-Healing lub PPR,
* Partial Cache Line Sparing
 |
| **Gniazda PCI** | * minimum jeden slot PCIe
 |
| **Interfejsy sieciowe/SAS** | * Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
 |
| **Dyski twarde** | Zainstalowane minimum:* 2x dysk SSD SATA o pojemności minimum 480GB, 6Gb, 2,5“ Hot-Plug.
* 2x dysk SAS o pojemności minimum 2.4TB, 12Gb, 2,5“ Hot-Plug.
* Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności minimum 480GB z możliwością konfiguracji RAID 1.
* Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
 |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1,10
 |
| **Wbudowane porty** | * Przednie: minimum 1x VGA, minimum 1x USB 2.0, minimum 1x micro-USB dedykowane dla karty zarządzającej,
* Tylne: minimum. 1x VGA, minimum 2x USB w tym 1x USB 3.0,
 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
 |
| **Zasilacze** | * Redundantne, Hot-Plug maksymalnie 700W klasy Titanium
 |
| **System operacyjny/dodatkowe oprogramowanie** | Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie Wszystkie core oferowanych procesorów. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
* Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
 |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
* Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
 |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o:
* Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
* Przesyłanie danych telemetrycznych w czasie rzeczywistym
* Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
* Automatyczna rejestracja certyfikatów (ACE)
 |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
* integracja z Active Directory
* Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
* Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
* Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
* Szczegółowy opis wykrytych systemów oraz ich komponentów
* Możliwość eksportu raportu do CSV, HTML, XLS, PDF
* Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
* Grupowanie urządzeń w oparciu o kryteria użytkownika
* Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
* Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
* Szybki podgląd stanu środowiska
* Podsumowanie stanu dla każdego urządzenia
* Szczegółowy status urządzenia/elementu/komponentu
* Generowanie alertów przy zmianie stanu urządzenia.
* Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
* Integracja z service desk producenta dostarczonej platformy sprzętowej
* Możliwość przejęcia zdalnego pulpitu
* Możliwość podmontowania wirtualnego napędu
* Kreator umożliwiający dostosowanie akcji dla wybranych alertów
* Możliwość importu plików MIB
* Przesyłanie alertów „as-is” do innych konsol firm trzecich
* Możliwość definiowania ról administratorów
* Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
* Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
* Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
* Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
* Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
* Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
* Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
* Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
* Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
* Zdalne uruchamianie diagnostyki serwera.
* Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
* Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V
 |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:Monitoring:* ilość podłączonych oraz rozłączonych systemów
* stan podłączonych urządzeń
* informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
* Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
* informacje o statusie gwarancji dla poszczególnych urządzeń
* informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
* informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
* Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
* Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
* Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
* Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
* Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
* Monitoring parametrów serwerów z informacją o minimum:
* Obciążeniu procesora
* Zużyciu pamięci RAM
* Temperaturze procesorów
* Temperaturze powietrza wlotowego
* Zużyciu prądu
* Zmianach w fizycznej konfiguracji serwera
* Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
* Monitoring parametrów pamięci masowych z informacją o minimum:
* Opóźnieniach
* IOPS
* Przepustowości
* Utylizacji kontrolerów
* Pojemność całkowita i dostępna
* Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
* Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
* Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
* Informacje o poziomie redukcji danych
* Informacje o statusie replikacji oraz snapshotów
* Monitoring parametrów przełączników sieciowych z informacją o minimum:
* Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
* Stanie komponentów: zasilacze, wentylatory
* Podłączonych hostach
* Ilości i statusu portów
* Utylizacji procesora
* Utylizacji poszczególnych portów
* Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
 |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub normami równoważnymi,
* Serwer musi posiadać deklaracja CE lub równoważną
* Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Wykonawca powinien załączyć oświadczenie producenta potwierdzające spełnianie wymogu
* Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku (wydruk należy załączyć do oferty).
 |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
* Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
 |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 miesięcy.
* Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
* Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)
* Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
* Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
* Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
* Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
* Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
* Zamawiający wymaga dołączenia do oferty oświadczenia od producenta sprzętu lub autoryzowanego Partnera Serwisowego Producenta , że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
* Serwis urządzeń musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
* Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

Zamawiający wymaga dołączenia do oferty oświadczenia od producenta sprzętu potwierdzające, że serwis oferowanego serwera będzie: - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; - firma serwisująca posiada autoryzacje producenta oferowanego serwera; - firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. |
| **Wymagania dodatkowe** | W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług: * Konfiguracja serwera:
	+ stworzenie planu wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie serwera wirtualizacyjnego w wskazanej przez Zamawiającego szafie rack.
	+ montażu w/w sprzętu w szafie rack w sposób zgodny z zaleceniami producenta dostarczanych serwerów.

Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera.* + podłączenia serwera do wskazanej przez Zamawiającego infrastruktury sieciowej za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera
	+ wykonać testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania.
* Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.
* Wymaga się, aby Wykonawca w ramach dostawy serwera zapewnił dostęp do urządzenia kryptograficznego spełniającego wymagania FIPS-140 Level minimum 3. Urządzenie to może być dostępne dla Zamawiającego jako urządzenie w Cloud z gwarancją przechowywania kluczy kryptograficznych na terenie Polski, lub jako osobne urządzenie w formie karty PCIe lub osobnego urządzenia dostępnego z poziomu sieci LAN.

Na potrzeby udostępnienia takiej usługi Wykonawca musi zapewnić osobny slot urządzenia kryptograficznego na wyłączne potrzeby Zamawiającego. Wymagane interfejsy komunikacji z urządzeniem kryptograficznym PKCS#11, CSP/CNG. Komunikacja sieciowa pomiędzy siedzibą Zamawiającego a urządzeniem kryptograficznym musi być zaszyfrowana za pomocą połączenia IPSEC z kluczem szyfrującym o długości minimum 256bitów typu AES. Dopuszczalne jest użycie algorytmu ECC o długości 192bitów. |
| **Ilość** | 1 szt.  |

## Serwer typ 3 (rozbudowa serwera AD)

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Serwer typ 3 (rozbudowa serwera AD). |
| **Wymagania szczegółowe** | Zamawiający do posiadanego serwera Fujitsu RX200 S7 o numerze seryjnym YLAQ020315 wymaga dostarczenia minimum:* 2 dysków HD SAS 6G 900GB 10K HOT PL 2.5' EP
* Systemu operacyjnego spełniającego wymagania w zakresie minimum: Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie wszystkie core oferowanych procesorów.

Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.* 130 licencji dostępowych dla Użytkowników
 |
| **Ilość** | 1 komplet  |

## Macierz do klastra

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Macierz do klastra |
| **Typ obudowy** | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji minimum 24 dysków 2.5” |
| **Przestrzeń dyskowa** | Zainstalowane minimum:* 12x dyski SAS o pojemności minimum 2.4TB, Hot-Plug
* 4x dyski SSD SAS o pojemności minimum 1.92TB, Hot-Plug
 |
| **Możliwość rozbudowy** | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych. |
| **Obsługa dysków** | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| **Sposób zabezpieczenia danych** | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| **Tryb pracy kontrolerów macierzowych** | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| **Pamięć cache** | Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| **Rozbudowa pamięci cache** | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| **Interfejsy** | Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler) |
| **Kable/wkładki** | Minimum: 4x kabel 12Gb HD Mini-SAS/HD Mini-SAS minimum 2m |
| **Zarządzanie** | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| **Zarządzanie grupami dyskowymi oraz dyskami logicznymi** | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Thin Provisioning** | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Tiering** | Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |
| **Wewnętrzne kopie migawkowe** | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Wewnętrzne kopie pełne** | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| **Migracja danych w obrębie macierzy** | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| **Podłączanie zewnętrznych systemów operacyjnych** | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| **Redundancja** | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold. |
| **Dodatkowe wymagania** | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| **Standardy bezpieczeństwa** | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) lub normy równoważne |
| **Inne** | Sprzęt powinien być wyprodukowany zgodnie z normami ISO 9001 oraz ISO 14001.Deklaracja zgodności CE. |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:Monitoring:* ilość podłączonych oraz rozłączonych systemów
* stan podłączonych urządzeń
* informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
* Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
* informacje o statusie gwarancji dla poszczególnych urządzeń
* informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
* informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
* Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
* Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
* Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
* Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
* Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
* Monitoring parametrów serwerów z informacją o minimum:
* Obciążeniu procesora
* Zużyciu pamięci RAM
* Temperaturze procesorów
* Temperaturze powietrza wlotowego
* Zużyciu prądu
* Zmianach w fizycznej konfiguracji serwera
* Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
* Monitoring parametrów pamięci masowych z informacją o minimum:
* Opóźnieniach
* IOPS
* Przepustowości
* Utylizacji kontrolerów
* Pojemność całkowita i dostępna
* Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
* Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
* Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
* Informacje o poziomie redukcji danych
* Informacje o statusie replikacji oraz snapshotów
* Monitoring parametrów przełączników sieciowych z informacją o minimum:
* Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
* Stanie komponentów: zasilacze, wentylatory
*  Podłączonych hostach
* Ilości i statusu portów
* Utylizacji procesora
* Utylizacji poszczególnych portów
* Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

Aktualizacja firmware* możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
* możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania

Raporty* Możliwość generowania raportów dla serwerów zawierających informację o:
* Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
* Średnim obciążeniu: procesorów, pamięci RAM, IO,
* Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
* Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
* Generowanie raportów do plików CSV i PDF

Cyberbezpieczeństwo* Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
* Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
* Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
* Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.

Wspierane urządzenia* Urządzenie Producenta dostarczane w ramach postępowania
* Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)

Wirtualny asystent* Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;

Możliwość rozszerzenia funkcjonalności* Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.

Inne* Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

CertyfikatyOferowana platforma musi być zaprojektowana zgodnie ze standardami:* ISO 27001
* NIST Security and Privacy Controls for Federal Information Systems and Organization
* CSA Cloud Control Matrix
 |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 miesięcy.
* Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
* Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)
* Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
* Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
* Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
* Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
* Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
* Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego (do oferty należy załączyć oświadczenie producenta oferowanej macierzy lub autoryzowanego Partnera Serwisowego Producenta potwierdzające, że oferowana macierz posiada gwarancję w ramach której, w przypadku wystąpienia awarii dysku twardego w oferowanej macierzy, uszkodzony dysk twardy pozostaje u Zamawiającego).
* Zamawiający wymaga usługi diagnostyki sprzętu na miejscu w przypadku awarii. Zamawiający oczekuje możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie Zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z Producentem w celu uzyskania pomocy. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
* Serwis urządzeń musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
* Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń

Zamawiający wymaga dołączenia do oferty oświadczenia od producenta sprzętu potwierdzające, że serwis oferowanej macierzy będzie: - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta; - firma serwisująca posiada autoryzacje producenta oferowanej macierzy; - firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. |
| **Wymagania dodatkowe** | W ramach dostawy Zamawiający wymaga dodatkowo wdrożenia w zakresie minimum: * inicjalizacja wstępna,
* aktualizacja firmware kontrolerów i dysków,
* montaż fizyczny u klienta,
* adresacja IP zgodnie z uzgodnieniami z Zamawiającym,
* utworzenie volumenów zgodnie z wymaganiami Zamawiającego,
* podłączenie SAS z hostami,
* udostępnienie zasobów dla hostów,
* konfiguracja migawek volumenów,
* szkolenie z podstawowej obsługi macierzy,
* przygotowanie dokumentacji powdrożeniowej.
 |
| **Ilość** | 1 sztuka |

## UPS do serwerowni

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS do serwerowni  |
| **Technologia** | VFI (true on-line, podwójne przetwarzanie energii) |
| **Budowa** | Beztransformatorowa, prostownik IGBT.UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i Bypassu. |
| **Wymagania ogólne** | UPS z możliwością konfiguracji wejścia/wyjścia w układzie: 3:3 lub 3:1Moc znamionowa minimum: 10kVA/10kWWyjściowy współczynnik mocy (PF): 1,0Współczynnik mocy wejściowej: 0.99. 0,99Napięcie wejściowe trójfazowe: 400 VAC 3F + NTolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie: 167 – 288 Vac (L-N)Zakres częstotliwości wejściowej: Wymagana 40-70 HzSprawność AC-AC w trybie pracy on-line z obciążeniem 100%: nie mniejsza niż 96%Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza Możliwość rozbudowy mocy w systemie równoległym okresie eksploatacji do minimum: 3 sztuk w układzie pracy równoległejWymagany jest montażu modułu pracy równoległej w oferowanej jednostce pozwalający na dołączenie kolejnej jednostkiNapięcie wyjściowe trójfazowe lub jednofazowe: 400 VAC 3F + N / 230 VAC 1FCzęstotliwość wyjściowa: 50/60Hz (programowalna)Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass): Statyczny przełącznik (SCR) oraz ręczny rozłącznik serwisowyWejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przełącznika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przełączeniem Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniemMożliwość regulacji prądu ładowania baterii z poziomu panelu LCD w UPS-ieCzas podtrzymania minimum: 32 minut przy obciążeniu 6kWLokalizacja baterii: Baterie umieszczone w module UPSa oraz zewnętrznej szafie bateriiBaterie szczelne AGM VRLA o żywotności minimum 10 latAutonomia pracy zasilacza UPS przy pracy z baterii podawana w minutach na panelu LCD zasilaczaWyświetlacz LCD kolorowy, dotykowy, z menu w języku polskimW przypadku uszkodzenia pojedynczych akumulatorów w stosie, wymagana poprawna praca urządzenia ze zmniejszonym łańcuchem baterii poprzez konfiguracjęStabilizacja napięcia wyjściowego w stanie ustalonym: ± 1%Stabilizacja napięcia wyjściowego w stanie nieustalonym: ± 3%Stabilność częstotliwości wyjściowej: bez synchronizacji: ± 0,05 HzWspółczynnik szczytu 3:1Minimalne przeciążenie falownika w trybie pracy normalnej • 110% przez 60 minut• 125% przez 10 minut• 150% przez 1 minutęPanel sterujący z wyświetlaczem dotykowym oraz sygnalizacją akustyczną Złącze interfejsów minimum: USB, RS232, SNMP, Porty pracy równoległej.Karta sieciowa SNMP wbudowana w UPSInterfejs EPO (do wyłącznika ppoż.): UPS zintegrowany z systemem ppoż budynku.Diagnostyka parametrów urządzenia UPS i baterii: automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-aPoziom hałasu w odległości 1m: <58 dBARejestr zdarzeń: Dziennik zdarzeń w UPS-ie oraz komunikaty serwisoweMożliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassuUPS wyposażony w zdalny wyłącznik REPOSpełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE lub normami równoważnymi dla UPS i baterii Certyfikat ISO 9001 i 14001 dystrybutora i producenta sprzętu lub z normami równoważnymi Zasilacz UPS musi być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPSa. Wymaga się co najmniej czterech rozłączników zamontowanych na UPS: zasilanie prostownika, zasilanie bypass, bypass serwisowy, rozłącznik wyjściowy z UPS.Podłączenie zasilania i odbiorów: podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego.Zasilacz musi być wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji Zewnętrzny bypass serwisowy wyposażony w pojedynczy przełącznik do bezprzerwowego przełączenia zasilania pomiędzy UPS-SIEĆ Instrukcja w języku polskim  |
| **Gwarancja** | Minimum 24 miesięcy producenta, z zastrzeżeniem, że baterie o żywotności minimum 10 lat |
| **Ilość** | 1 sztuka |

## Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 (przełącznik) |
| **Wymagania ogólne**  | Przełącznik zarządzalny minimum 48portowy.* Przełącznik wielowarstwowy: L3
* Obsługa jakość serwisu (QoS) : Tak
* Zarządzanie przez stronę www: Tak
 |
| **Obudowa** | * Możliwość montowania w stelażu.
* Możliwość Stackowania
* Układ max 1U
* Przepływ powietrza z boku na bok
 |
| **Porty i interfejsy** | * Podstawowe przełączanie RJ-45 Liczba portów Ethernet: min 48
* Podstawowe przełączania Ethernet RJ-45 porty typ: Gigabit Ethernet (10/100/1000)
* Ilość slotów Modułu SFP+ : min. 4
* Port konsoli : RJ-45/micro-USB
 |
| **Wydajność przełącznika** | * Wirtualne układanie (w szt.): minimum 8
* Procesor wbudowany: Tak
* Taktowanie procesora: min. 1016 MHz
* Typ pamięci: min DDR3-SDRAM
* Pojemność pamięci wewnętrznej: min. 1024 MB
* Wielkość pamięci flash: min 4096 MB
 |
| **Protokoły** | * Protokoły zarządzające: SNMPv1, SNMPv2, SNMPv3, Telnet, RMON1, FTP
* Protokół wybierania drogi: RIPng, VRRP
* Funkcje IPv4 i IPv6 : IPv4/IPv6 access-control list (ACL)
 |
| **Sieć** | * Standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1v, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3az, IEEE 802.3u, IEEE 802.3x
* Obsługa 10G: Tak
* Półdupleks: Tak
* przekierowywanie IP : Tak
* Protokół drzewa rozpinającego : Tak
* Automatyczne wykrywanie : Tak
* Limit częstotliwości : Tak
* Automatyczne MDI/MDI-X: Tak
* Agregator połączenia: Tak
* Obsługa sieci VLAN: Tak
* Funkcje wirtualnej sieci LAN: Private VLAN
 |
| **Przesyłanie danych** | * Przepustowość rutowania/przełączania: minimum 178 Gbit/s
* Przepustowość: minimum 112 Mpps
* Wielkość tabeli adresów: minimum 32768 wejścia
* Latency (1 Gbps): maksimum 3,8 µs
* Latency (10 Gbps): maksimum1,6 µs
* Pamięci bufora pakietów: minimum 12 MB
 |
| **Ochrona** | * Lista kontrolna dostępu (ACL): Tak
* Typ uwierzytelniania: RADIUS, TACACS+
* obsługuje SSH/SSL: Tak
* Uwierzytelnianie oparte na MAC, Uwierzytelnianie przez Internet
 |
| **Moc** | * Źródło zasilania: Prąd przemienny
* Zasilacz dołączony: Tak
* Napięcie wejściowe AC: 100 - 240 V
* Częstotliwość wejściowa AC: 50/60 Hz
* Maksymalne zużycie mocy: 47 W
 |
| **Warunki Pracy** | * Zakres temperatur (eksploatacja): 0 - 45 °C
* Zakres temperatur (przechowywanie): -40 - 70 °C
* Zakres wilgotności względnej: 15 - 95%
* Dopuszczalna wilgotność względna: 15 - 95%
* Emisja ciepła: Maksymalnie 158 BTU/h
 |
| **Wymagania dodatkowe** | Zamawiający wymaga dostarczenia min. 4 szt. wkładek optycznych SFP kompatybilnych z oferowanym przełącznikiem |
| **Gwarancja** | Min. 12 miesięcy producenta |
| **Ilość** | 1 sztuka |

## Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 (rozbudowa posiadanych przełączników)  |
| **Wymagania szczegółowe** | W ramach rozbudowy posiadanych przez Zamawiającego przełączników: switcha HP Aruba 5400E zl2 o numerze seryjnym SG02G4913XY, Zamawiający wymaga dostawy modułu SFP oraz wkładek w zakresie minimum: * min. 1 szt. Modułu 8xSFP+ : Aruba 8-Port 1G/10GbE SFP+ v3 zl2
* min. 4 szt. wkładek optycznych SFP+ 10km
* min. 4 szt. wkładek optycznych SFP 20km
 |
| **Gwarancja** | Minimum 12 miesięcy producenta |
| **Ilość** | 1 komplet |

## Oprogramowanie do wykonywania kopii zapasowych

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie do wykonywania kopii zapasowych |
| **Wymagania szczegółowe** | **1. Wymagania ogólne:**Oprogramowanie powinno mieć możliwość używania w dwóch scenariuszach:* Cloud (Software as Service),
* On-premise.

Powinna istnieć możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.Interfejs systemu oraz pomoc techniczna powinna być dostępna w języku:* polskim,
* angielskim,Oprogramowanie powinno mieć możliwość uruchamiania w kontenerze docker,

Oprogramowanie powinno mieć możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy operacyjne.System powinien wykonywać kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,Oprogramowanie powinno działać w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju),**2. Wsparcie techniczne:**Pomoc techniczna w językach:* polskim,
* angielskim.

Materiały samopomocowe:* Baza wiedzy: polski, angielski

**3. Zarządzanie:**Zarządzanie całością działania systemu (backup, przywracanie) powinno być z poziomu jednej konsoli webowej,Zarządzanie całym systemem powinno być poprzez dashboardy,Gradacja uprawnień kont administratorów powinna być z poziomu panelu zarządzającego,System powinien posiadać wbudowane predefiniowane zadania backupowe,System powinien umożliwiać tworzenie zadań backupowych w oparciu o kalendarz.System powinien umożliwiać automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,System powinien umożliwiać automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,System powinien umożliwiać monitorowanie postępu działania zadania,System powinien posiadać powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:* Zadanie zostało zakończone pomyślnie,
* Zadanie zostało zakończone z ostrzeżeniami,
* Zadanie zostało zakończone z błędem,
* Zadanie zostało anulowane,
* Zadanie nie zostało uruchomione.

System powinien generować alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.System powinien umożliwiać możliwość zdefiniowania okna backupowego dla każdego z zadań,Oprogramowanie powinno posiadać wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,System powinien pozwalać na klonowanie planów kopii zapasowych,System powinien umożliwiać reset hasła administratora w przypadku jego utraty,Oprogramowanie powinno umożliwiać definiowanie retencji według schematów:* GFS (Grandfather-Father-Son),
* FIFO (First-In, First-Out).

Oprogramowanie powinno umożliwiać tworzenie kont użytkowników nie będących administratorami,System powinien umożliwiać tworzenie kont użytkowników poprzez import pliku CSV,Oprogramowanie powinno umożliwiać tworzenie grup urządzeń,Oprogramowanie powinno zapewniać zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).System powinien pozwalać na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:* System Administrator,
* Backup operator,
* Restore operator,
* Viewer.

**4. Składowanie danych:**Oprogramowanie powinno być systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,System powinien umożliwiać składowanie danych:* Lokalnie:Zasób SMB,Zasób NFS,Zasób ISCSI,Zasób S3,Katalog zabezpieczonego urządzenia.
* W chmurze:Amazon Web Service,Magazyn zgodny z S3,Dostarczanej przez producenta.

System powinien pozwalać na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,System powinien posiadać mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.System powinien umożliwiać replikacje danych między magazynami. **5. Odtwarzanie:**System powinien umożliwiać odtwarzanie granularne:* Pojedynczych plików z kopii obrazu dysku,
* Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,

System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:* Windows: 7 i wyższe,
* Windows Server: 2008 R2 i wyższe,

Odtwarzanie Bare metal Restore powinno odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.Uruchamianie procesu Bare Metal Restore powinno odbywać się z bootowalnej płyty CD lub pendrive’a,Oprogramowanie powinno umożliwiać odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.Oprogramowanie powinno umożliwiać odtwarzanie kopii obrazu dysku w wybranym formacie (VHD, VHDX, VMDK),System powinien umożliwiać odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),System powinien umożliwiać odtwarzanie zasobów plikowych z prawami dostępu,System powinien umożliwiać Przywracanie plików pomiędzy systemami operacyjnymi (np. odtwarzanie danych plikowych Linux na systemie Windows),System powinien umożliwiać odtwarzanie danych według harmonogramu,System powinien umożliwiać przywracanie danych z określonego urządzenia/użytkownika,System powinien umożliwiać przywracanie kopii z wybranego magazynu.System powinien posiadać możliwość nieodwracalnego kasowania danych,System powinien umożliwiać przywracanie repozytoriów GIT:* Przywracanie pomiędzy hostingami repozytoriów (GitHub/BitBucket),
* przywracanie między kontami.

**5. Backup:**Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla Systemów operacyjnych.* Środowisk wirtualnych.
* Repozytoriów GIT.

Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla Baz danych..Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:* 128 bit,
* 192 bit,
* 256 bit.

Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:* ZStandard,
* LZ4.

Oprogramowanie powinno umożliwiać zarządzanie poziomem kompresji,System powinien umożliwiać wykonywanie kopii zapasowej otwartych plików(VSS),System powinien umożliwiać uruchamianie skryptów przed i po backupie,System powinien umożliwiać uruchamianie skryptów po wykonaniu migawki VSS,System powinien umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,System powinien umożliwiać backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,System powinien umożliwiać backup plikowy,Oprogramowanie powinno realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,Oprogramowanie powinno umożliwiać konsolidację wersji kopii zapasowych,Oprogramowanie powinno zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,Oprogramowanie powinno pozwalać na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.Oprogramowanie powinno pozwalać na backup zaszyfrowanych partycji. Oprogramowanie powinno zapewniać wsparcie dla repozytoriów lokalnych oraz zdalnych (dostępnych w usługach zewnętrznych),Oprogramowanie powinno umożliwiać zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki). |
| **Licencjonowanie** | Licencje powinny pozwalać na zabezpieczenie w opcji wieczystej :* 100 stacji roboczych
* 2 serwerów fizycznych bez wirtualizacji,
* Nielimitowanej ilości maszyn wirtualnych w obrębie 2 fizycznych serwerów stanowiących podstawy do wirtualizacji (łącznie 4 socketów)

Wsparcie techniczne:* Powinno być świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,
* Zapewnia dostęp do aktualizacji oprogramowania,
* Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,
* Obowiązuje przez okres minimum 12 miesięcy.
 |
| **Ilość** | 1 komplet |

## 11. Oprogramowanie SIEM Security Information and Event Management

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie SIEM Security Information and Event Management |
| **Wymagania ogóle** | Platforma przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności, spełniająca wymagania minimalne:1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi. 2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding. 3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach. 4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI; 5. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. 6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie. 7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych. 9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware. 10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. 11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji. 12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX. 13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora. 14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej. 15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B. 16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie. 17. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów. 18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe. 19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej. 20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych. 21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach. 22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.  23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.  24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.  25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej. 26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług. 27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły. 28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.  29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: a) nowe zasoby wykryte w sieci, b) typy wykrytych zasobów (np.: serwer lub stacja robocza), c) zastosowane na nich zabezpieczenia, d) usługi z którymi się komunikują, e) nowe usługi wykryte na zasobie f) komunikację do usług wykrytych na zasobie. 30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację. 31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora. 32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy. 33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników: a) fqdn, b) e-mail, c) nazwa pliku, d) ścieżka do pliku, e) hash, f) adres IP, g) klucz rejestru, h) cmd. 34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/). 35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu). 36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”). 37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych. 38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. 39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np.: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu). 40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT. 41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu. 42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie. 43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności: a) id techniki, b) taktykę, c) platformy których dotyczy, d) potencjalne źródła, e) opis zagrożenia, f) mityzację, g) sposób detekcji, h) referencje. 44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. 45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy). 46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: a) rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, b) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, c) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, d) rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów. 47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA). 48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji. 49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet). 50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. 51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację. 52. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: a) sparsowane pola oraz ich wartości, b) listy referencyjne, c) atrybuty użytkowników z Active Directory, d) atrybuty komputerów z Active Directory, e) bazę wskaźników kompromitacji (IOC), f) informacje z elektronicznej dokumentacji, g) anomalie w zachowaniu użytkowników (UBA), h) anomalie w zachowaniu zasobów (EBA), i) podatności na zasobach, j) wyniki analizy konfiguracji, k) techniki MITRE ATT&CK®, 53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić: a) wykrycie dowolnej treści w logach, b) wykrycie zmiany jednego z kilku pól, c) wykrycie zaniku wiadomości, d) wykrycie nowej wartości pola w zadanym okresie czasu, e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu, m) wykrycie skanowania portów. 54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: a) wykrycie wystąpienia wartości pola na wybranej liście, b) wykrycie niewystępowania wartości pola na wybranej liście, c) wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony), d) wykrycie niewystąpienia pary wartości na wybranej liście e) np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył). 55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, c) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej. 56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej. 57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji; b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji; 58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, c) wykrycie nieautoryzowanej usługi na serwerze, d) wykrycie nieautoryzowanego połączenia do usługi na serwerze, e) wykrycie nieautoryzowanego połączenia z serwera usług, f) wykrycie nieautoryzowanego połączenia do sieci Internet. 59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN. 60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach. 61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, c) wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności, d) wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności. 62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na: a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić: a) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, b) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, c) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie. 64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.: a) wykrycie anomalii na koncie uprzywilejowanym użytkownika, b) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, c) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, d) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, e) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać: a) sparsowane pola oraz ich wartości, b) atrybuty użytkowników z Active Directory, c) atrybuty komputerów z Active Directory, d) informacje z elektronicznej dokumentacji. 66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: a) adresie IP, b) koncie domenowym użytkownika, c) strefie bezpieczeństwa, d) zakresie adresów IP. 67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej. 68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze. 69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in. a) wszystkie skorelowane zdarzenia, b) korespondencja pocztowa, c) załączniki z próbkami lub dowodami, d) wskaźniki kompromitacji (IoC), e) informacje pozyskane z innych systemów. 70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora. 71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa. 72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: a) identyfikację celu i źródła zagrożenia, b) nazwę oraz adres IP źródła zagrożenia, c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, d) lokalizację z które pochodzi zagrożenie np.: Internet, e) strefę bezpieczeństwa z której pochodzi zagrożenie, f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), h) nazwę oraz adres IP celu zagrożenia, i) zabezpieczenia lokalne chroniące cel zagrożenia, j) strefę bezpieczeństwa w której znajduje się cel zagrożenia. 73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall). 74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem. 75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: a) nazwy zasobu, b) rodzaju zasobu, c) ważności zasobu dla organizacji, d) rodzaj przetwarzanych informacji, e) usług, które ten zasób świadczy, f) lokalizację użytkowników, którzy z niego korzystają, g) usługi z których zasób korzysta. 76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych. 77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: a) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, b) segregacja – segregacja i kwalifikacja zdarzeń, c) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, d) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, e) zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”. 78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi. 79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych. 80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów. 81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów. 82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów. 83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API. 84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: a) podgląd aktywności zagrożonego zasobu na linii czasu, b) w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, c) w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, d) podgląd reguły korelacyjnej, która wygenerowała zdarzenie, e) w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis, f) listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, g) gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o: • listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, • listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym, f) gotowe i proste w użyciu filtry rozszerzajcie analizę logów o: • listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, • listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym. 85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a) warunki powiadomień, • zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, • zdarzeń o przekroczonych czasach SLA o definiowalny okres, • zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, • zdarzeń, których priorytet osiągnął określoną wartość, • zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, • zdarzeń na których doszło do naruszenia bezpieczeństwa, • zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, • zdarzeń realizujących zdefiniowaną usługę, • zdarzeń przetwarzających sklasyfikowane informację, • zdarzeń przetwarzanych na krytycznych zasobach, b) odbiorców powiadomień, w tym: • operatora, któremu zostało przydzielone zdarzenie, • właściciela zasobu na którym wystąpiło zdarzenie, • zespół obsługi, który odpowiada za obsługę zdarzeń, • właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie, • podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną. c) kanały powiadomień, m.in. e-mail, sms, komunikator, d) zastosowanie mechanizmów grupowania: • grupowanie wielu powiadomień w jednej wiadomości, • ograniczenie liczby wierszy powiadomienia do określonej wartości. 86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a) utworzenia nowego zdarzenia z określonym priorytetem, b) utworzenia nowego zdarzenia na zasobie krytycznym, c) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, d) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, e) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, f) modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, g) zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, h) przejęcia przydzielonego operatorowi zdarzania przez innego operatora. 87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: a) wybór raportu, który ma zostać wysłany, b) zdefiniowanie jego tytułu, c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d) możliwość ograniczenia cyklu do dni powszednich, e) określenie daty przesłania pierwszego raportu, f) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do: • zdefiniowanej daty końcowej, • określnej liczby raportów, g) określenie odbiorców raportu. 88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook). 89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry: a) strefę bezpieczeństwa w której została wykryta podatność, b) prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, c) rodzaj zasobu którego dotyczy ta podatność, d) ważność tego zasobu dla organizacji, e) przetwarzane na tym zasobie informacje, np.: dane osobowe, f) usługi realizowane przez ten zasób, np.: DNS, g) wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High, h) poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, i) szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet. 90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji. 91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: a) wyliczonym priorytecie podatności, b) aktualnym statusie obsługi, c) ważności zasobu na którym została wykryta, d) adresie IP tego systemu, e) parametrów SLA związanych z tym statusem, f) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, g) parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”. 92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach: a) przekroczenia czasu reakcji o określony czas np.: o godzinę, b) możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, c) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, d) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, e) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, f) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, g) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, h) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, i) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, j) przekroczenia czasu reakcji dla podatności na zasobie krytycznym, k) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę, 93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a) warunki powiadomień• podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, • podatności o przekroczonych czasach SLA o definiowalny okres, • podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, • podatności, których priorytet osiągnął określoną wartość, • zdarzeń realizujących zdefiniowaną usługę, • zdarzeń przetwarzających sklasyfikowane informację, • zdarzeń przetwarzanych na krytycznych zasobach, b) odbiorców powiadomień, w tym: • operatora, któremu została przydzielona podatność, • właściciela zasobu na którym wystąpiła podatność, • zespół obsługi, który odpowiada za obsługę podatności, • właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność, • podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną. c) kanały powiadomień, m.in. e-mail, sms, komunikator, d) zastosowanie mechanizmów grupowania: • grupowanie wielu powiadomień w jednej wiadomości, • ograniczenie liczby wierszy powiadomienia do określonej wartości. 94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a) przydzielenia nowej podatności do obsługi z określonym priorytetem, b) przydzielenia nowej podatności do obsługi na zasobie krytycznym, c) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, d) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, e) modyfikacji przydzielonej operatorowi podatności przez innego operatora, f) zamknięcia przydzielonej operatorowi podatności przez innego operatora, g) przejęcia przydzielonej operatorowi podatności przez innego operatora. 95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na: a) wybór raportu który ma zostać wysłany, b) zdefiniowanie jego tytułu, c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d) możliwość ograniczenia cyklu do dni powszednich, e) określenie daty przesłania pierwszego raportu, f) określenie okresu przez jaki będą one przesyłane, poprzez: • zdefiniowanie daty końcowej, • bez daty końcowej, • określenie liczby raportów, g) określenie odbiorców raportu. 96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika. 97. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących: a) zestaw wykresów dla bieżącego użytkownika, b) zestaw wykresów dla wybranego użytkownika, c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center). 98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy: a) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia: • ilość zdarzeń nowych i niesklasyfikowanych, • ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa, • ilość zdarzeń sklasyfikowanych jako fałszywe alarmy, b) wykres przedstawiający skale zagrożeń, który uwzględnia: • ilość zasobów krytycznych na których są obsługiwane zdarzenia, • ilość zasobów niekrytycznych na których są obsługiwane zdarzenia, c) wykres przedstawiający źródła zagrożeń, który uwzględnia: • ilość nowych zdarzeń dotyczących użytkowników, • ilość podjętych zdarzeń dotyczących użytkowników, • ilość nowych zdarzeń dotyczących zasobów, • ilość podjętych zdarzeń dotyczących zasobów, d) wykres przedstawiający poziom zagrożeń, który uwzględnia: • ilość nowych zdarzeń w podziale na priorytety, • ilość podjętych zdarzeń w podziale na priorytety, e) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia: • ilość zdarzeń zarejestrowanych w bieżącym dniu, • ilość zdarzeń zarejestrowanych w ostatnim tygodniu, • ilość zdarzeń zarejestrowanych w ostatnim miesiącu, • ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu, f) wykres przedstawiający zagrożone usługi, który uwzględnia: • ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, • ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia, g) wykres przedstawiający zagrożone dane, który uwzględnia: • ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, • ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, h) wykres przedstawiający skale podatności, który uwzględnia: • ilość zasobów krytycznych na których są obsługiwane podatności, • ilość zasobów niekrytycznych na których są obsługiwane podatności, i) wykres przedstawiający czas obsługi podatności, który uwzględnia: • ilość podatności zarejestrowanych w bieżącym dniu, • ilość podatności zarejestrowanych w ostatnim tygodniu, • ilość podatności zarejestrowanych w ostatnim miesiącu, • ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu, j) wykres przedstawiający wagę podatności, który uwzględnia: • ilość nowych podatności w podziale na priorytety, • ilość podjętych podatności w podziale na priorytety, 99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie: a) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, b) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, c) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, d) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, e) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, f) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres. 100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. 101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych: a) kolektor parsujący; b) kolektor logów; c) kolektor korelacyjny; d) kolektor zdarzeń; e) kolektor sztucznej inteligencji; f) kolektor reakcyjny; g) kolektor kontrolujący. 102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń. 103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń. 104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. 105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). 106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody. 107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji. 108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych. 109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe. 110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania. 111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów. 112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej. 113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów. 114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.) 115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych. 116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych. 117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta. 118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania. 119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji. 120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB). 121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania. 122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów 123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI) 124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI). 125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości: a) zdolność do definiowania wzorców które powtarzają się jako zmienne; b) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych; c) zdolność do testowania poszczególnych funkcji; d) zdolność do przekształcania danych w trakcie ich parsowania. 126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości: a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej; b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; d) zdolność do monitorowania integralności plików; e) zdolność do monitorowania rejestru systemowego; f) zdolność do monitorowania urządzeń zewnętrznych (removable devices); g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS; h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS; j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu. 127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar. 128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI 129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń. 130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data). 131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi 132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal. 133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł. 134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji. 135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów. 136. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM. 137. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego. 138. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć. 139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem. 140. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie. 141. Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać min 150 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności. 142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów. 143. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet. 144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).  |
| **Wymagania dotyczące licencji i wsparcia** | Dostarczone rozwiązanie musi być w formie licencji wieczystej oraz być objęte wsparciem producenta lub producentów minimum do 17.06.2026 r. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego). Zamawiający wymaga, aby dostarczone rozwiązanie posiadało interfejs w języku polskim, oraz aby wsparcie dostarczonego rozwiązania również było w języku polskim. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu. Wykonawca w ramach dostawy musi zapewnić bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla minimum 2 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez Certyfikowanego Inżyniera systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej. |
| **Ilość** | 1 szt.  |

## 12. Oprogramowanie do monitorowania infrastruktury informatycznej

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie do monitorowania infrastruktury informatycznej |
| **Wymagania ogólne** | W ramach dostawy Zamawiający wymaga rozbudowy i przedłużenia serwisów do posiadanego rozwiązania eAuditor. Wymagane jest upgrade do wersji V8 professional, rozszerzenie do 120 użytkowników oraz rozszerzenie o funkcjonalność skaner maszyn wirtualnych. Licencje i serwisy mają obowiązywać do daty 17.06.2026 r.Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne. Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo: - wdrożenia - skonfigurowania dla wszystkich użytkowników - przeszkolenia administratorów dostarczonego oprogramowania, wg ustaleń z Zamawiającym. |
| **OPIS RÓWNOWAŻNOŚCI – wymagania minimalne:** |
| **Wymagania funkcjonalne** | **1. Architektura / budowa**1.1. System musi umożliwić bezproblemową i stabilną obsługę minimum 120 Klientów jednocześnie. System musi mieć menu w języku polskim. 1.2. Architektura / budowa:1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.1.3. Konfiguracja Architektury:1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.**2. Wymagania systemowe**2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server, Windows 10/11, Linux, macOS2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, FireFox2.3. Serwer musi działać na systemach 64 bitowych: Windows Server, Windows 10/11.2.4. Serwer www musi być oparty o platformę Microsoft 64 bit Windows Server, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.2.5. Baza danych musi działać na silniku Microsoft SQL Server w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.**3. Interfejsy**3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.3.2. System musi umożliwiać import danych z CSV3.3. System zapewnia integrację z modelem LLM.**4. Funkcjonalności systemu zarządzania infrastrukturą IT**4.1. Funkcjonalność Klienta4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.4.2. Funkcjonalność konsoli administracyjnej.4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń. 4.3. Funkcjonalność panelu pracownika4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.4.4. Zarządzanie licencjami4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.4.5. Wzorce aplikacji i pakietów4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.4.7. Inwentaryzacja urządzeń sieciowych.4.7.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.4.8. Inwentaryzacja sprzętu.4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.4.9. Ochrona danych (DLP)4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.4.10. Zdalna administracja komputerami4.10.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.4.11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.4.12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.4.13. Zdalne Zarządzanie Zaporą (Firewall)4.13.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.4.14. Automatyzacja4.14.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.4.15. Zarządzanie magazynem IT4.15.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.4.16. Repozytorium4.16.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.4.17. Kody kreskowe4.17.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.4.18. Wysyłanie wiadomości4.18.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.4.19. System musi posiadać możliwość eksportu / importu treści.4.20. Monitorowanie drukarek sieciowych i wydruków4.20.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.4.21. Monitorowanie stron www4.21.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.4.22. Monitorowanie serwerów WWW4.22.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.4.23. Monitorowanie dziennika zdarzeń4.23.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.4.24. System musi umożliwiać monitorowanie komunikatów Syslog.4.25. Monitorowanie pracy komputerów4.25.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.4.26. Monitorowanie sensorów4.26.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.4.27. Repozytorium CMDB4.27.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.4.28. Worktime manager4.28.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.4.29. Raportowanie i eksport danych4.29.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.4.30. System musi zapewnić interfejs API.4.30.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki. 4.31. Powiadomienia4.31.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.4.32. Bezpieczeństwo4.32.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych. **5. Wsparcie i pomoc** 5.1.1. Pomoc techniczna 5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. Musi być świadczona w języku polskim. 5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.5.1.1.3. Czas trwania usługi SLA: do17.06.2026 r. |
| **Ilość** | 1 szt.  |

# Obszar kompetencyjny

## 1. Szkolenia typ 1 (Szkolenia dla pracowników z działu IT)

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkoleń** |
| **Typ** | Szkolenia typ 1 (Szkolenia dla pracowników z działu IT) |
| **Szkolenie z Oprogramowania do monitorowania infrastruktury informatycznej** | Wykonawca zapewni szkolenie (minimum 8h) dla administratorów Zamawiającego (2 osoby) z posiadanego przez Zamawiającego rozwiązania do monitorowania sieci - eAuditor. Szkolenie w formie zdalnej. Szkolenie obejmuje w zakresie minimum: 1. Przygotowanie oraz wysłanie konfiguracji- Opis wszystkich dostępnych sekcji- Przygotowanie konfiguracji dla eAgentów według zaleceń klienta.- Wysłanie przygotowanej konfiguracji do zainstalowanych eAgentów.2. Instalacja i aktualizacja oprogramowania.- Pobranie instalatora eAgenta- Instalacja eAgenta na końcówkach.- Podłączenie do eServera oraz sprawdzenie między nimi komunikacji.3. Autoryzacja eAgenta.- Przygotowanie komputera do autoryzacji- Omówienia statusów autoryzacji4. Wymuszenie skanowania.- Wymuszenie skanowania na wszystkich końcówkach z eAgentami – tak, aby zebrały się dane według nowych ustawień.5. Integracja systemu z Active Directory- Import danych w zakresie:- Struktur organizacyjnych- Osób- Uprawnień administracyjnych6. Konfiguracja użytkowników eWebConsole, nadanie praw dostępu.- Zakładanie nowych użytkowników- Tworzenie grup użytkowników- Nadawanie uprawnień w zakresie struktur organizacyjnych i widoków.7. Zarządzanie automatami w Serwerze automatyzacji- Konfiguracja- Automatycznych zadań- Automatycznych zdarzeń- Automatycznej konserwacji8. Kopia bezpieczeństwa.- Konfiguracja automatycznej:- Kopii- Konserwacji (shrink)- Reindeksacji bazy danych9. Filtrowanie danych- Filtry kolumnowe- Filtr ogólny- Filtr widoku- Filtr globalny10. Zarządzanie komputerami w systemie eAuditor- Przebieg autoryzacji.- Cel autoryzacji.- Ewidencja komputerów.- Zasoby komputera.- Czas pracy komputera.- Kolejki wydruków.- Logowanie użytkowników.- Urządzenia USB.11. Serwer zadań w systemie eAuditor- Zadania CMD i PowerShell predefiniowane.- Zadania użytkownika.- Przedstawienie działania blokowania urządzeń USB na zasadzie „Białej listy”.- Przygotowanie testowej reguły i prezentacja zastosowania.12. Zarządzanie urządzeniami w systemie eAuditor- Skaner sieci.- Dodawanie urządzeń.- Przypisywanie użytkowników do urządzeń.- Inwentaryzacja sprzętu – kody kreskowe.13. Zarządzanie oprogramowaniem w systemie- eAuditor:- Audyt legalności oprogramowania- Audyt multimediów- Schematy oprogramowania- Wzorce oprogramowania- Ewidencja licencji oraz dokumentów licencyjnych (załączniki elektroniczne).- Śledzenie różnic w plikach i rejestrach.- Definiowanie oprogramowania zabronionego, zalecanego, dodatkowego.- Edycja i zamawianie wzorców14. Serwer wiadomości w systemie eAuditor:- Komunikacja z użytkownikami.- Wiadomości jednorazowa.- Cykliczne wiadomości.- Automatyczne planowanie szkoleń.15. Raportowanie w systemie eAuditor:- Generowanie raportów.- Harmonogram raportów- Raporty statyczne i dynamiczne oparte na Crystal Reports.- Automatyzacja i dystrybucja raportów na maila.16. Powiadomienia w systemie eAuditor- Konfiguracja powiadomień: Alert, e – mail, sms17. MagazynSzkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. 12 miesięcy, jednak nie później niż do dnia 17.06.2026 r. |
| **Szkolenie z utworzenia usługi katalogowej w formie warsztatów** | Wykonawca zapewni szkolenie z zakresu Microsoft Active Directory posiadanego przez Zamawiającego (minimum 1 dzień, 8 h) dla administratorów Zamawiającego (2 osoby). Szkolenie w formie zdalnej. Szkolenie musi odbyć się w formie warsztatowej na środowisku przygotowanym przez Wykonawcę. Program szkolenia będzie obejmować w zakresie minimum: Moduł 1: Instalacja i konfiguracja kontrolerów domeny * Omówienie usług AD DS
* Omówienie kontrolerów domeny usług AD DS
* Wdrożenie kontrolera domeny

Moduł 2: Zarządzanie obiektami w AD DS * Zarządzanie kontami użytkowników
* Zarządzanie grupami w usługach AD DS
* Zarządzanie obiektami typu komputer w AD DS
* Wdrażanie i zarządzanie OU

Moduł 3: Wdrażanie i zarządzanie lokacjami i repliką AD DS * Omówienie replikacji usług AD DS
* Konfigurowanie lokacji usług AD DS
* Konfigurowanie i monitorowanie replikacji usług AD DS

Moduł 4: Wdrażanie zasad grupy * Wprowadzenie do zasad grupy
* Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)
* Konfiguracja zakresu i przetwarzania obiektów GPO
* Rozwiązywanie problemów z GPO

Moduł 5: Zarządzanie ustawieniami użytkowników za pomocą zasad grupy * Wdrażanie szablonów administracyjnych
* Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
* Konfiguracja preferencji zasad grupowych

Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. 12 miesięcy, jednak nie później niż do dnia 17.06.2026 r. |
| **Szkolenie z konfiguracji przełączników** | Wykonawca zapewni szkolenie z zakresu przełączników Aruba posiadanych przez Zamawiającego (minimum 3 dni, 8h lekcyjnych dziennie, łącznie 24 godziny lekcyjne) dla administratora Zamawiającego (1 osoba). Szkolenie w formie zdalnej. Szkolenie będzie obejmować w zakresie minimum:* Wprowadzenie do Aruby, firmy Hewlett Packard Enterprise
* Opisanie trendów rynkowych, które powodują transformację klientów w czterech kluczowych obszarach transformacji
* Przedstawienie, w jaki sposób Aruba zapewnia cyfrowe miejsce pracy
* Przełączanie nawigacji CLI (interfejs wiersza poleceń).
* Przedstawienie zarządzania poza pasmem
* Przeprowadzenie wstępnej konfiguracji przełączników ArubaOS
* Sprawdzenie konfiguracji
* Ochrona dostępu do zarządzania
* Wyjaśnienie zarządzania wewnątrz pasma
* Ochrona dostępu do zarządzania w paśmie i poza pasmem
* Skonfigurowanie uwierzytelniania lokalnego
* Kontrolowanie poziomu uprawnień przyznany menedżerom
* Zarządzanie oprogramowaniem i konfiguracjami
* Przegląd systemu ArubaOS i struktur plików
* Różne metody ustawiania oprogramowania, z którego ma zostać uruchomiony system
* Aktualizacja oprogramowania
* Zapisywanie i przywracanie konfiguracji
* VLANY
* Wyjaśnienie przypadków użycia sieci VLAN
* Konfiguracja sieci VLAN oparte na portach na przełącznikach ArubaOS, używając odpowiedniego tagowania
* Wdrożenie podstawowego routingu IP pomiędzy bezpośrednio podłączonymi sieciami VLAN lub łączami
* Protokół drzewa opinającego (STP)
* Przedstawienie i skonfigurowanie protokołu Rapid Spanning Tree Protocol (RSTP)
* Przedstawienie w jaki sposób protokół MSTP (Multiple Spanning Tree Protocol) zapewnia podział obciążenia i zaimplementuj protokół MSTP
* Agregacja łącza
* Rozróżnienie różnych typów agregacji łączy i oraz przedstawienie zalet protokołu kontroli agregacji łączy (LACP)
* Konfigurowanie i rozwiązywanie problemów z agregacją łączy na przełącznikach ArubaOS
* Trasowanie IP
* Konfiguracja tras statycznych na przełącznikach ArubaOS
* Interpretacja tablic routingu IP
* Konfiguracja podstawowych rozwiązań OSPF
* Wirtualna struktura przełączania (VSF)
* Omówienie jak działa VSF i jakie korzyści zapewnia
* Konfiguracja i weryfikacja prostej struktury VSF
* Bezprzewodowość dla małych i średnich firm (SMB)
* Wyjaśnienie podstaw komunikacji bezprzewodowej i standardów 802.11
* Zdefiniowanie sieć WLAN i rozróżnienie opcji zabezpieczeń sieci bezprzewodowej
* Konfigurowanie podstawowe ustawienia Aruba Instant Access Point (IAP)
* Utworzenie klastra Aruba Instant
* Aruba AirWave
* Konfiguracja ustawienia zarządzania AirWave w klastrze IAP
* Konfiguracja ustawienia SNMP v2c na przełącznikach ArubaOS
* Przełączniki ArubaOS w AirWave, monitorowanie i zarządzanie przełącznikami oraz IAP
* Wdrożenie obsługi bezdotykowej (ZTP) dla punktów IAP firmy Aruba i przełączników ArubaOS

Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. 12 miesięcy, jednak nie później niż do dnia 17.06.2026 r. |
| **Szkolenie z oprogramowania do backupu** | Wykonawca zapewni szkolenie z zakresu oprogramowania do backupu wdrażanego w punkcie I.10 niniejszej specyfikacji (minimum 6 h) dla administratora Zamawiającego (1 osoba). Szkolenie w formie zdalnej. Szkolenie będzie obejmować w zakresie minimum: * Omówienie ekosystemu rozwiązania do backupu
* Podstawy backupu
* omówienie różnych rodzajów backupu: pełny, różnicowy, przyrostowy
* Przedstawienie kluczowych terminów związanych z backupem: RPO, RTO, polityka retencji
* Zajęcia praktyczne z rozwiązania do backupu
* Wdrożenie XMS
* Instalacja agenta
* Przykładowa konfiguracja planów backupowych
* Omówienie dobrych praktyk backupowych
* Testowanie backupu
* Zarządzanie backupem

Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. 12 miesięcy, jednak nie później niż do dnia 17.06.2026 r. |
| **Szkolenie z cyberbezpieczeństwa** | Wykonawca zapewni szkolenie z zakresu cyberbezpieczeństwa (minimum 2 h) dla administratora Zamawiającego (2 osoby). Szkolenie w formie zdalnej. Szkolenie będzie obejmować w zakresie minimum: * Podstawowe przedstawienie zagadnienia cyberbezpieczeństwa
* Przedstawienie zagrożeń, które czyhają na nas w sieci (rodzaje zagrożeń i ich konsekwencje)
* Opis i wymagania normy ISO/IEC 27001
* Dlaczego wiedza o cyberbezpieczeństwie jest konieczna
* Sposoby ochrony kont i danych przed potencjalnym zagrożeniem.
* Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności a co za tym idzie programy pomagające w tym
* Logowanie w sieci.
* Opis Certyfikatów stron internetowych.
* Darmowe WiFi i automatyczne podłączanie się.
* Wprowadzenie do sieci komputerowych - niebezpieczeństwo sieci otwartych bezprzewodowych
* Praca zdalna - czym jest VPN i jak z niego korzystać.
* Programy antywirusowe i ich rola (omówienie popularnych programów i opis ich działania)
* Tworzenie kopii zapasowych i ich odzyskiwanie po awarii.
* Niezabezpieczone protokoły sieciowe - HTTP FTP
* Zaszyfrowana komunikacja w Internecie
* Ochrona plików i dysków, czyli podstawy szyfrowania.
* Fizyczne aspekty bezpieczeństwa cybernetycznego - jak zabezpieczenie fizyczne urządzeń i systemów wpływa na cyberbezpieczeństwo.
* Bezpieczeństwo urządzeń mobilnych i Internetu Rzeczy (IoT) - przedstawienie wyzwań i metod zabezpieczenia urządzeń połączonych z internetem, w tym smartfonów, smartwatchy, i urządzeń domowych.
* Zarządzanie tożsamością i dostępem - omówienie metod uwierzytelniania, w tym uwierzytelnianie wieloskładnikowe (MFA), zarządzanie tożsamością i dostępem (IAM), i ich znaczenie dla ochrony danych i systemów.

Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie w okresie min. 12 miesięcy, jednak nie później niż do dnia 17.06.2026 r. |
| **ilość** | 1 komplet  |