**Załącznik nr 1 do SWZ**

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

|  |
| --- |
|  |

Spis treści

[Wstęp 2](#_Toc1959679919)

[I. WYMAGANIA OGÓLNE 4](#_Toc861008790)

[1 RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ 4](#_Toc243632150)

[II. Obszar techniczny 5](#_Toc2045111578)

[1. UTM (Unified Threat Management) 5](#_Toc1802281533)

[2. Serwer 14](#_Toc1906199456)

[3. Macierz dyskowa 26](#_Toc965132203)

[4. Network Attached Storage NAS typ 1 33](#_Toc439569944)

[5. Oprogramowanie SIEM Security Information and Event Management 36](#_Toc1546494123)

[III. Obszar kompetencyjny 66](#_Toc1045161919)

[1. Szkolenia dla działu IT typ 1 66](#_Toc1211226369)

[2. Szkolenia dla działu IT typ 2 69](#_Toc1489803987)

# Wstęp

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Kożuchów 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.

# WYMAGANIA OGÓLNE

## RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ

#### w zakresie Oprogramowania

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, zapewnić gwarancję i serwis, uwzględnić niezbędną asystę ze strony pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Mając na uwadze powyższe, w przypadku jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności, przejrzystości, jawności a także równego traktowania wykonawców w trakcie prowadzenia postępowania, Zamawiający dopuszcza każdorazowo wymianę Oprogramowania u Zamawiającego pod warunkiem, że:

* + - * 1. Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt, z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.
        2. Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, w sposób opisany w niniejszym OPZ a migracja musi objąć pełny zakres danych bieżących i archiwalnych.
        3. Wykonawca przeprowadzi instruktaże stanowiskowe, zapewni gwarancje i serwis gwarancyjny a także help desk oraz będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom Zamawiającego płynną obsługę Oprogramowania.
        4. Wymiana Oprogramowania nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.
        5. Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.
        6. Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.
        7. Nowe rozwiązania muszą realizować wszystkie wymienione wymagania względem Oprogramowania.

#### w zakresie Infrastruktury sprzętowej

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis: “Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 176 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.” należy rozumieć jako: “Zainstalowane co najmniej dwa procesory, posiadające co najmniej 8 rdzeni, co najmniej 2.9GHz, umożliwiające osiągnięcie wyniku co najmniej 176 w teście SPECrate2017\_int\_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej. “

# Obszar techniczny

## UTM (Unified Threat Management)

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie typu UTM |
| **Wymagania szczegółowe** | OBSŁUGA SIECI  1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.  ZAPORA KORPORACYJNA (Firewall)  2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.  3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.  4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).  5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.  6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.  7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.  8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.  9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.  10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.  11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).  12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.  INTRUSION PREVENTION SYSTEM (IPS)  13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.  14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.  15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.  16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.  17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.  18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.  19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.  20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.  21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).  22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.  23. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu  KSZTAŁTOWANIE PASMA (Traffic Shapping)  24. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.  25. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.  26. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).  27. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.  OCHRONA ANTYWIRUSOWA  28. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).  29. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.  30. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym  31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.  32. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.  OCHRONA ANTYSPAM  33. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).  34. Ochrona antyspam ma działać w oparciu o:  a. białe/czarne listy,  b. DNS RBL,  c. Skaner heurystyczny.  35. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.  36. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.  WIRTUALNE SIECI PRYWATNE (VPN)  37. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).  38. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:  a. PPTP VPN,  b. IPSec VPN,  c. SSL VPN.  39. SSL VPN ma działać co najmniej w trybach tunelu i portalu.  40. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.  41. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)  42. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).  43. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.  44. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.  FILTR DOSTĘPU DO STRON WWW  45. Urządzenie ma posiadać wbudowany filtr URL.  46. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu  47. Administrator ma mieć możliwość dodawania własnych kategorii URL.  48. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:  a. blokowanie dostępu do adresu URL,  b. zezwolenie na dostęp do adresu URL,  c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.  49. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.  50. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.  51. Filtr URL musi uwzględniać komunikację po protokole HTTPS.  52. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.  53. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.  54. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch  UWIERZYTELNIANIE  55. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:  a. lokalną bazę użytkowników (wewnętrzny LDAP),  b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),  c. usługę katalogową Microsoft Active Directory.  56. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.  57. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:  a. SSL,  b. Radius,  c. Kerberos.  58. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.  59. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.  60. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.  61. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).  62. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).  63. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.  ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)  64. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).  65. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:  a. równoważenie względem adresu źródłowego,  b. równoważenie względem połączenia.  66. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.  67. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).  68. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.  69. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).  70. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.  ROUTING (TRASOWANIE)  71. Urządzenie ma umożliwiać statyczne trasowanie pakietów.  72. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.  73. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).  74. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.  ADMINISTRACJA URZĄDZENIEM  75. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.  76. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.  77. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.  78. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.  79. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  80. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)  81. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.  82. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.  83. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.  84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.  85. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.  86. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).  87. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).  88. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.  89. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.  90. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).  91. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.  92. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:  a. manualnego eksportu do pliku w dowolnym momencie czasu,  b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu  93. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.  94. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.  95. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.  RAPORTOWANIE  96. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.  97. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.  98. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.  99. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.  100. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.  101. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.  102. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.  103. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.  104. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).  POZOSTAŁE USŁUGI I FUNKCJE  105. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.  106. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.  107. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).  108. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.  109. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).  110. Urządzenie ma posiadać usługę DNS Proxy.  111. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).  112. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.  113. Urządzenie musi mieć zaimplementowane Open API  114. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.  GWARANCJA I SERWIS  115. Urządzenie ma być objęte gwarancją producenta do 30.06.2026 roku na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.  116. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.  117. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny  PARAMETRY SPRZĘTOWE  118. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.  119. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.  120. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.  121. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.  122. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:  a. Moduł z 8 interfejsami miedzianymi 2,5Gbps  b. Moduł z 4 interfejsami miedzianymi 10Gbps.  c. Moduł z 4 interfejsami światłowodowymi 1Gbps.  d. Moduł z 8 interfejsami światłowodowymi 1Gbps.  e. Moduł z 4 interfejsami światłowodowymi 10Gbps.  123. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.  124. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.  125. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.  126. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.  127. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.  128. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.  129. Maksymalna liczba tuneli VPN IPSec – minimum 1000.  130. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.  131. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.  132. Obsługa interfejsów 802.11q (VLAN) – minimum 256.  133. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.  134. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.  135. Urządzenie nie ma limitu na liczbę użytkowników.  136. Liczba reguł filtrowania – minimum 16 384.  137. Liczba tras statycznego routingu – minimum 5 120.  138. Liczba tras dynamicznego routingu – minimum 10 000.  139. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.  Urządzenie musi być wyposażone w moduł TPM. |
| **Wymagania dodatkowe** | Zamawiający w ramach dostawy wymaga wdrożenia w zakresie minimum:   * Urządzenie należy zamontować w miejscu wskazanym przez Zamawiającego. * Urządzenie musi być zaadresowanie zgodnie z przedstawionymi wymaganiami przekazanymi na etapie wdrożenia. Minimalne wymaganie wdrożeniowe to 4vlany, 2 łącza wan, 2 tunele ipsec, 2 tunele SSL VPN. * Przygotowanie polityk NAT oraz Firewall w ilości minimum 10sztuk. * Wymianie podlegać musi obecnie posiadane urządzenie obsługujące ruch sieciowy jednostki.Wymiana musi zostać wykonana w czasie po godzinach pracy jednostki (lub innym uzgodnionym terminie). * Na dzień wdrożenia urządzenie musi posiadać najnowszy firmware wraz z aktualnymi sygnaturami. * Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania, który będzie potwierdzeniem posiadania umiejętności min: (Certyfikat należy załączyć do oferty) * Sieci i routingu w dostarczonym rozwiązaniu * Przechwytywania i analizy ruchu sieciowego * Konfiguracji i diagnostyki połączeń IPSec VPN oraz SSL VPN * Konfiguracji systemu IPS oraz dostosowywania jego konfiguracji * Konfiguracji i analizy polityk bezpieczeństwa * Konfiguracji mechanizmu NAT * Konfiguracji uwierzytelniania użytkowników * Kontroli dostępu do stron WWW oraz deszyfrowania ruchu sieciowego w celu analizy przez systemy bezpieczeństwa * Konfiguracji i diagnostyki mechanizmów zapewniania wysokiej dostępności * Konfiguracji mechanizmów PKI w dostarczonym rozwiązaniu * Przeszukiwania logów dotyczących ruchu sieciowego oraz pracy urządzenia * Wsparcia technicznego i rozwiązywania problemów z dostarczonym rozwiązaniem |
| **Ilość** | 1 szt. |

## Serwer

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Sprzęt serwerowy wraz z niezbędnym oprogramowaniem do stworzenia klastra wysokiej dostępności |
| **Obudowa** | * Obudowa Rack o wysokości max 1U z możliwością instalacji 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 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. * Obsługa procesorów 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 min. 8-rdzeniowe, min. 2.9GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 176 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Wynik testu dołączyć do oferty. |
| **RAM** | Minimum 384GB DDR5 RDIMM 5600MT/s, |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10 |
| **Dyski twarde** | * Zainstalowane minimum:   + 2x dysk SSD SATA o pojemności min. 480GB Hot-Plug.   Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | Minimum trzy sloty PCIe LP |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * Minimum czteroportowa karta 12Gb SAS HBA |
| **Wbudowane porty** | * Minimum 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * Minimum 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | Redundantne, Hot-Plug min. 700W klasy Titanium |
| **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 |
| **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 minimum 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. |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * 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 lub równowaznymi. 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 oraz integrację z posiadaną platformą wirtualizacji VMware. 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 aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji 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 * Certyfikaty   + Oferowana platforma musi być zaprojektowana zgodnie ze standardami:     - ISO 27001 lub równoważne     - NIST Security and Privacy Controls for Federal Information Systems and Organization lub równoważne     - CSA Cloud Control Matrix lub równoważne |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne * Serwer musi posiadać deklaracja CE lub równoważne . * Serwer musi spełniać wymagania normy NIST SP 800-193 lub równoważnej ochrony przed cyberatakami. Wykonawca powinien załączyć do oferty 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * 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, że posiada on gwarancję w ramach której w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, 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 lub równoważne 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 wymaga montażu fizycznych serwerów wraz z pełną aktualizacją systemu operacyjnego hosta i maszyn wirtualnych/oprogramowania układowego serwera na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego i 2 maszyn wirtualnych które to Wykonawca musi uruchomić na w/w serwerze. Parametry minimalne w/w maszyn wirtualnych zostaną podane na etapie realizacji wdrożenia.  W ramach wdrożenia należy podłączyć oba dostarczane serwery do dostarczanej macierzy za pomocą dedykowanych przewodów. Zezwala się na połączenie direct między macierzą i serwerem bez wykorzystania dedykowanego przełącznika.  W ramach wdrożenia należy wykonać testy redundancji sieci SAN za pomocą fizycznego odpięcia każdej ścieżki.  Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania serwerem.  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** | 2szt |

## Macierz dyskowa

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Macierz pamięci masowej |
| **Typ obudowy** | Macierz musi być przystosowana do montażu w szafie rack 19”,  o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5” |
| **Przestrzeń dyskowa** | Zainstalowane:  Minimum 8x dysk SSD SAS o pojemności min. 3.84TB, 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 min. 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 równoważne |
| **Inne** | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym  producenta |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. 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 aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizcji 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 * Certyfikaty   + Oferowana platforma musi być zaprojektowana zgodnie ze standardami:     - ISO 27001 lub równoważne     - NIST Security and Privacy Controls for Federal Information Systems and Organization lub równoważne     - CSA Cloud Control Matrix lub równoważne |
| **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 i przez Internet.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  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 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, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:  • 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.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
| **Wymagania dodatkowe** | Zamawiający wymaga montażu macierzy wraz z pełną aktualizacją systemu operacyjnego hosta /oprogramowania układowego macierzy na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania. Na etapie wdrożenia należy przewidzieć zasób Quorum dla zbudowania klastra wysokiej dostępności z wykorzystaniem powyższej macierzy.  W ramach wdrożenia należy podłączyć macierzy za pomocą dedykowanych przewodów. Zezwala się na połączenie direct między macierzą i serwerem bez wykorzystania dedykowanego przełącznika.  W ramach wdrożenia należy wykonać testy redundancji sieci SAN za pomocą fizycznego odpięcia każdej ścieżki.  Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania macierzą. |
| **ilość** | 1 sztuka |

## Network Attached Storage NAS typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie typu NAS |
| **Procesor** | Procesor 64-bitowy x86 o takowaniu nie mniejszym niż 2,9 GHz |
| **Procesor liczba rdzeni** | Nie mniej niż 6 |
| **Pamięć RAM** | Nie mniej niż 32 GB ECC DDR4 |
| **Pamieć RAM liczba slotów** | Minimum 4 sloty |
| **Pamięć RAM - możliwość rozszerzenia** | Nie mniej niż do 128 GB |
| **Pamięć Flash** | Nie mniej niż 5 GB |
| **Liczba zatok na dyski** | Minimum 18 w tym min. 12 x 3,5-calowych SATA oraz min. 6 x 2,5-calowych SATA |
| **Ilość zainstalowanych dysków** | Minimum 5szt x 14TB | 7200 RPM | SATA 6Gb/s and SAS 12Gb/s  Minimum 2 szt x Dysk SSD 1TB M.2 NVMe pod cache |
| **Obsugiwane dyski twarde** | 3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD |
| **Pojemność dysków twardych** | do 22TB |
| **Możliwość podłączenia modułu rozszerzającego** | Tak, co najmniej 2 |
| **Porty LAN 2,5 GbE** | Minimum 2 |
| **Porty LAN 10 GbE** | Minimum 2 |
| **Diody LED** | Minimum Stan, LAN, stan dysku, USB |
| **Porty USB 3.2 Gen2** | Minimum 4 x typu A |
| **Port PCiE** | Tak, minimum 3 |
| **Przyciski** | Reset, Zasilanie |
| **Typ obudowy** | RACK, 2U |
| **Dopuszczalna temperatura pracy** | od 0 do 40˚C |
| **Wilgotność względna podczas pracy** | 5-95% R.H. |
| **Zasilanie** | Zasilacz redundatny 2 x max 550 W, 100-240 V |
| **Obsługa dwóch systemów operacyjnych** | Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS |
| **Agregacja łączy** | Tak |
| **Obsługiwane systemy plików** | Dyski wewnętrzne: EXT4  Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT |
| **Możliwość podłączenia karty WLAN na USB** | Tak |
| **Szyfrowanie udziałów** | Tak, min AES 256 |
| **Szyfrowanie dysków zewnętrznych** | Tak |
| **Zarządzanie dyskami** | Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD,  Obsługa Hot Spare per grupa RAID oraz global hot spare  Rozszerzanie pojemności Online RAID  Migracja poziomów Online RAID  HDD S.M.A.R.T.  Skanowanie uszkodzonych bloków  Przywracanie macierzy RAID  Obsługa map bitowych  Pula pamięci masowej  Obsługa migawek  Obsługa replikacji migawek |
| **Wbudowana obsługa iSCSI** | Multi-LUNs na Target  Obsługa LUN Mapping & Masking  Obsługa SPC-3 Persistent Reservation  Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN |
| **Zarządzanie prawami dostępu** | Ograniczenie dostępnej pojemności dysku dla użytkownika  Importowanie listy użytkowników  Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie współdzieleniem w sieci  Tworzenie użytkowników za pomocą makr  Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL |
| **Obsługa Windows AD** | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web  Funkcja serwera LDAP |
| **Funkcje backup** | Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, |
|  |  |
| **Darmowe aplikacje na urządzenia mobilne** | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer  Dostępne na systemy iOS oraz Android |
| **Minimum obsługiwane serwery** | Serwer plików  Serwer FTP  Serwer WEB  Serwer kopii zapasowych  Serwer multimediów UPnP  Serwer pobierania (Bittorrent / HTTP / FTP)  Serwer Monitoringu |
| **VPN** | VPN client / VPN server  Obsługa PPTP, OpenVPN |
| **Administracja systemu** | Połączenia HTTP/HTTPS  Powiadamianie przez e-mail (uwierzytelnianie SMTP)  Powiadamianie przez SMS  Ustawienia inteligentnego chłodzenia  DDNS oraz zdalny dostęp w chmurze  SNMP (v2 & v3)  Obsługa UPS z zarządzaniem SNMP (USB)  Obsługa sieciowej jednostki UPS  Monitor zasobów  Kosz sieciowy dla CIFS/SMB oraz AFP  Monitor zasobów systemu w czasie rzeczywistym  Rejestr zdarzeń  Całkowity rejestr systemowy (poziom pliku)  Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line  Aktualizacja oprogramowania automatyczna  Możliwość aktualizacji oprogramowania ręcznie  Ustawienia systemu: Kopia, Przywracanie, Resetowanie |
| **Wirtualizacja** | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.  Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5  Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. |
| **Konteneryzacja** | Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |
| **Zabezpieczenia** | Filtracja IP  Ochrona dostępu do sieci z automatycznym blokowaniem  Połączenie HTTPS  FTP z SSL/TLS (Explicit)  Obsługa SFTP (tylko admin)  Szyfrowanie AES 256-bit  Szyfrowana zdalna replikacja (Rsync poprzez SSH)  Import certyfikatu SSL  Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| **Możliwość instalacji dodatkowego oprogramowania** | Tak, sklep z aplikacjami; możliwość instalacji z paczek |
| **Wymagania dodatkowe** | Zamawiający wymaga dostarczenia wraz z urządzeniem kartę posiadającą parametry w zakresie minimum:  Złącze: minimum 2 gniazda M.2 lub NVMe SSD SATA PCIe (Gen3 x 4)  PCIe i szyny: minimum PCIe Gen3 x 4  Uchwyt: Niskoprofilowy, wraz z dodatkowymi uchwytami: niskoprofilowy płaski i pełnej wysokości. |
| **Wymagania wdrożeniowe** | Zamawiający wymaga aby w ramach dostarczenia urządzenia NAS zostały wykonane następujące czynności:   * + montaż zamówionych dysków w zatokach urządzenia,   + aktualizacja oprogramowania systemowego urządzenia,   + montaż fizyczny we wskazanej przez Zamawiającego szafie Rack,   + podłączenie fizyczne i adresacja IP zgodnie z wytycznymi Zamawiającego,   + utworzenie grupy dysków,   + utworzenie Volumenów zgodnie z wytycznymi Zamawiającego,   + dokumentacja powdrożeniowa. |
| **Gwarancja** | Minimum 60 miesięcy producenta |
| **Ilość** | 1 szt. |

## 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:   1. nowe zasoby wykryte w sieci, 2. typy wykrytych zasobów (np.: serwer lub stacja robocza), 3. zastosowane na nich zabezpieczenia, 4. Usługi, z którymi się komunikują, 5. nowe usługi wykryte na zasobie 6. 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:   1. fqdn, 2. e-mail, 3. nazwa pliku, 4. ścieżka do pliku, 5. hash, 6. adres IP, 7. klucz rejestru, 8. 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:   1. id techniki, 2. taktykę, 3. platformy których dotyczy, 4. potencjalne źródła, 5. opis zagrożenia, 6. mityzację, 7. sposób detekcji, 8. 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:   1. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, 2. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, 3. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, 4. 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:   1. sparsowane pola oraz ich wartości, 2. listy referencyjne, 3. atrybuty użytkowników z Active Directory, 4. atrybuty komputerów z Active Directory, 5. bazę wskaźników kompromitacji (IOC), 6. informacje z elektronicznej dokumentacji, 7. anomalie w zachowaniu użytkowników (UBA), 8. anomalie w zachowaniu zasobów (EBA), 9. podatności na zasobach, 10. wyniki analizy konfiguracji, 11. techniki MITRE ATT&CK®,   53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:   1. wykrycie dowolnej treści w logach, 2. wykrycie zmiany jednego z kilku pól, 3. wykrycie zaniku wiadomości, 4. wykrycie nowej wartości pola w zadanym okresie czasu, 5. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, 6. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, 7. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, 8. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, 9. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, 10. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, 11. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, 12. wykrycie ilości uruchomionych procesów w zadanym okresie czasu, 13. wykrycie skanowania portów.   54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:   1. wykrycie wystąpienia wartości pola na wybranej liście, 2. wykrycie niewystępowania wartości pola na wybranej liście, 3. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony), 4. wykrycie niewystąpienia pary wartości na wybranej liście 5. np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył).   55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:   1. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, 2. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, 3. 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). 4. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), 5. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.   56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:   1. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, 2. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, 3. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.   57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:   1. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji; 2. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; 3. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;   58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:   1. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, 2. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, 3. wykrycie nieautoryzowanej usługi na serwerze, 4. wykrycie nieautoryzowanego połączenia do usługi na serwerze, 5. wykrycie nieautoryzowanego połączenia z serwera usług, 6. wykrycie nieautoryzowanego połączenia do sieci Internet.     59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:   1. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 2. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, 3. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, 4. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.   60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:   1. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 2. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, 3. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, 4. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.   61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:   1. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, 2. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, 3. wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności, 4. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.   62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:   1. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, 2. 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:   1. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 2. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 3. 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.:   1. wykrycie anomalii na koncie uprzywilejowanym użytkownika, 2. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, 3. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, 4. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, 5. 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:   1. sparsowane pola oraz ich wartości, 2. atrybuty użytkowników z Active Directory, 3. atrybuty komputerów z Active Directory, 4. 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:   1. adresie IP, 2. koncie domenowym użytkownika, 3. strefie bezpieczeństwa, 4. 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.   1. wszystkie skorelowane zdarzenia, 2. korespondencja pocztowa, 3. załączniki z próbkami lub dowodami, 4. wskaźniki kompromitacji (IoC), 5. 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:   1. identyfikację celu i źródła zagrożenia, 2. nazwę oraz adres IP źródła zagrożenia, 3. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, 4. lokalizację z które pochodzi zagrożenie np.: Internet, 5. strefę bezpieczeństwa z której pochodzi zagrożenie, 6. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, 7. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), 8. nazwę oraz adres IP celu zagrożenia, 9. zabezpieczenia lokalne chroniące cel zagrożenia, 10. 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:   1. nazwy zasobu, 2. rodzaju zasobu, 3. ważności zasobu dla organizacji, 4. rodzaj przetwarzanych informacji, 5. usług, które ten zasób świadczy, 6. lokalizację użytkowników, którzy z niego korzystają, 7. 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:   1. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, 2. segregacja – segregacja i kwalifikacja zdarzeń, 3. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, 4. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, 5. 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:   1. podgląd aktywności zagrożonego zasobu na linii czasu, 2. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, 3. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, 4. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, 5. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis, 6. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, 7. 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,  1. 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:   1. 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,  1. 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.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. 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:   1. utworzenia nowego zdarzenia z określonym priorytetem, 2. utworzenia nowego zdarzenia na zasobie krytycznym, 3. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, 4. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, 5. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, 6. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, 7. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, 8. 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:   1. wybór raportu, który ma zostać wysłany, 2. zdefiniowanie jego tytułu, 3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 4. możliwość ograniczenia cyklu do dni powszednich, 5. określenie daty przesłania pierwszego raportu, 6. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:  * zdefiniowanej daty końcowej, * określnej liczby raportów,  1. 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:   1. strefę bezpieczeństwa w której została wykryta podatność, 2. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, 3. rodzaj zasobu, którego dotyczy ta podatność, 4. ważność tego zasobu dla organizacji, 5. przetwarzane na tym zasobie informacje, np.: dane osobowe, 6. usługi realizowane przez ten zasób, np.: DNS, 7. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High, 8. poprawność konfiguracji zasobu, na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, 9. 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:   1. wyliczonym priorytecie podatności, 2. aktualnym statusie obsługi, 3. ważności zasobu, na którym została wykryta, 4. adresie IP tego systemu, 5. parametrów SLA związanych z tym statusem, 6. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, 7. 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:   1. przekroczenia czasu reakcji o określony czas np.: o godzinę, 2. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, 3. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, 4. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, 5. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, 6. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, 7. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, 8. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, 9. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, 10. przekroczenia czasu reakcji dla podatności na zasobie krytycznym, 11. 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:   1. 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,  1. 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.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. 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:   1. przydzielenia nowej podatności do obsługi z określonym priorytetem, 2. przydzielenia nowej podatności do obsługi na zasobie krytycznym, 3. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, 4. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, 5. modyfikacji przydzielonej operatorowi podatności przez innego operatora, 6. zamknięcia przydzielonej operatorowi podatności przez innego operatora, 7. 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:   1. wybór raportu który ma zostać wysłany, 2. zdefiniowanie jego tytułu, 3. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 4. możliwość ograniczenia cyklu do dni powszednich, 5. określenie daty przesłania pierwszego raportu, 6. określenie okresu przez jaki będą one przesyłane, poprzez:  * zdefiniowanie daty końcowej, * bez daty końcowej, * określenie liczby raportów,  1. 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:   1. zestaw wykresów dla bieżącego użytkownika, 2. zestaw wykresów dla wybranego użytkownika, 3. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, 4. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).   98. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy:   1. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:  * ilość zdarzeń nowych i niesklasyfikowanych, * ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa, * ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,  1. wykres przedstawiający skale zagrożeń, który uwzględnia:  * ilość zasobów krytycznych na których są obsługiwane zdarzenia, * ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,  1. 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,  1. wykres przedstawiający poziom zagrożeń, który uwzględnia:  * ilość nowych zdarzeń w podziale na priorytety, * ilość podjętych zdarzeń w podziale na priorytety,  1. 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,  1. wykres przedstawiający zagrożone usługi, który uwzględnia:  * ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, * ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,  1. 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,  1. wykres przedstawiający skale podatności, który uwzględnia:  * ilość zasobów krytycznych na których są obsługiwane podatności, * ilość zasobów niekrytycznych na których są obsługiwane podatności,  1. 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,  1. 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:   1. „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, 2. „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, 3. „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, 4. „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, 5. „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, 6. „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:   1. kolektor parsujący; 2. kolektor logów; 3. kolektor korelacyjny; 4. kolektor zdarzeń; 5. kolektor sztucznej inteligencji; 6. kolektor reakcyjny; 7. 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:   1. zdolność do definiowania wzorców które powtarzają się jako zmienne; 2. zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych; 3. zdolność do testowania poszczególnych funkcji; 4. 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:   1. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej; 2. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; 3. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; 4. zdolność do monitorowania integralności plików; 5. zdolność do monitorowania rejestru systemowego; 6. zdolność do monitorowania urządzeń zewnętrznych (removable devices); 7. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS; 8. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; 9. 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; 10. 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 70 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 do 30.06.2026 roku. 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).  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. |
| **Wymagania dotyczące wdrożenia** | Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu.  Przedmiot Zamówienia będzie realizowany w oparciu o przygotowany uprzednio przez Wykonawcę Harmonogram Ramowy (rzeczowo-finansowy), który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram Ramowy w terminie 7 dni od daty podpisania umowy.  Wykonawca w Harmonogramie Ramowym musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.  Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad nie częściej niż jeden raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.    W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:   * Kierownik Projektu ze strony Wykonawcy, * Zespół Wdrożeniowy ze strony Wykonawcy.     W ramach wdrożenia rozwiązania SIEM Zamawiający wymaga, aby Wykonawca wdrożył rozwiązanie SIEM na minimum 2 maszynach wirtualnych przygotowanych przez Zamawiającego.  Zamawiający wymaga wdrożenia kompletnego systemu, w ramach którego zostanie podłączonych do 70 źródeł logów zgodnie z poniższą tabelą:     |  |  | | --- | --- | | Rodzaj usługi lub urządzenia | Liczba urządzeń / nodów będących źródłami logów | | Serwer | 5 szt. | | Macierz | 1 szt. | | Urządzenia klasy UTM | 1 szt. | | Usługa katalogowa | 2 szt. | | Przełączniki sieciowe | 8 szt. | | Punkty dostępowe | 2 szt. |     Wymaga się, aby Wykonawca przygotował harmonogram wdrożenia uwzględniający 6 etapów wdrożenia:   1. Analiza przedwdrożeniowa, 2. Instalacja systemu, 3. Konfiguracja systemu, 4. Dostrojenie systemu, 5. Szkolenia 6. Dokumentacja powdrożeniowa.     Wykonawca w ramach etapu 1 dokona analizy przedwdrożeniowej obejmującej wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie rozwiązania SIEM w środowisku informatycznym Zamawiającego. Analiza musi zawierać w szczególności:   1. Dane wstępne: 2. plan i sposób komunikacji Stron 3. harmonogram wdrożenia 4. Informacje o systemach bezpieczeństwa: 5. Analiza stanu bezpieczeństwa użytkowanych systemów przed rozpoczęciem realizacji projektu 6. Opis koniecznych działań dla osiągnięcia wymaganego stanu cyberbezpieczeństwa 7. Wymagane dane dotyczące systemów cyberbezpieczeństwa: 8. Wykonawca określi w Analizie przedwdrożeniowej optymalną konfigurację środowiska dla Systemu SIEM, m.in. pamięć, liczbę procesorów, wymagana powierzchnia dyskowa. 9. Dla każdego systemu cyberbezpieczeństwa Wykonawca opracuje:  * Wersję oprogramowania wchodzące w skład Systemu * Konfigurację Systemu * Zastosowane licencje/subskrypcje.  1. Procedura testowania – scenariusze testowe dla wdrażanych systemów 2. Harmonogram wdrożenia 3. Opis instalacji i wdrożenia oprogramowania     Wykonawca w ramach etapu 2 zainstaluje zaoferowane oprogramowanie według wcześniej przedstawionej architektury działania rozwiązania oraz wcześniej przygotowanego schematu komunikacji sieciowej w sieci lokalnej Zamawiającego.    Wykonawca w ramach etapu 3 zaimplementuje/skonfiguruje opracowane przez producenta reguły bezpieczeństwa wraz z weryfikacją ich działania dla konkretnych procesów określonych na etapie analizy przedwdrożeniowej.    Wykonawca w ramach etapu 4 dostroi system tak, aby nie powodował nadmiernej ilości fałszywych alarmów zaciemniających realne możliwe zagrożenia. Nie dopuszcza się sytuacji, w której jedno źródło logów spowoduję destabilizację działania całego systemu SIEM w krótkim okresie czasu np. 10minut.    Wykonawca w ramach etapu 5 przeprowadzeni szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 2 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez Certyfikowanego Inżyniera systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.  Wykonawca w ramach etapu 6 sporządzi i przekaże dokumentację powdrożeniową wskazującą wszystkie istotne elementy z punktu widzenia wdrożenia, wraz ze wszystkimi danymi dostępowymi do ewentualnych kont technicznych stworzonych na etapie wdrożenia.    Wykonawca po wdrożonym rozwiązaniu dokona następujących testów opisanych w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego.  Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.  W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.  Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze z zakresu:   * Uruchamianie i zatrzymywanie wdrożonego systemu. * Weryfikacja wdrożonego systemu zgodnie ze scenariuszami opisanymi w analizie przedwdrożeniowej. * Weryfikacja poprawności działania procedur. * Symulację awarii wdrożonego systemu. |
| **Świadczenie usługi SOC (Security Operations Center)** | Zamawiający wymaga, aby Wykonawca świadczył usługi SOC (Security Operations Center). przez okres minimum do końca trwania wsparcia producenta od systemu SIEM.    Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.    W ramach realizacji zadań Wykonawca będzie świadczył usługę administracji systemem SIEM obejmującą:   1. Informowanie Zamawiającego o awariach Systemu SIEM, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie, 2. Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa. 3. Optymalizowanie konfiguracji Systemu SIEM w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji. 4. Konfigurację Systemu SIEM w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego w Analizie Przedwdrożeniowej 5. Weryfikację czy System SIEM prawidłowo analizuje logi 6. Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.     W ramach usługi SoC Wykonawca będzie wysyłał Zamawiającemu informacje odnośnie pojawiających się podatności dla systemów wskazanych w ramach podłączonych źródeł logów.    W ramach realizacji zadań Wykonawca przygotuje i wdroży możliwe scenariusze wystąpienia incydentów bezpieczeństwa w systemie SIEM, które zostaną zaakceptowane przez Zamawiającego. Przykładowe scenariusze, które obligatoryjnie powinny być zaimplementowane:   * Bruteforce attack (atak siłowy) * Atak złośliwego oprogramowania (malware) * Atak typu DDoS * Wykrywanie usług sieciowych (Network Service Discovery) * Zdalne wykrywanie systemów (Remote System Discovery) * Pozyskiwanie informacji o systemie (System Information Discovery) * Interpreter poleceń i skryptów (Command and Scripting Interpreter)     W ramach realizacji zadań Wykonawca przygotuje i wdroży scenariusze reakcji rozumiane jako zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji powinien składać się z podzadań realizujących funkcje:   * **Wzbogacenia** wiedzy o artefaktach tj. adresy IP, domeny, hash’e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez udostępnione narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji, * **Analizy** zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia, * **Wydanie rekomendacji działań** rozumianej jako zestawienie rekomendacji umożliwiających ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym, * **Informowania i raportowania** obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.     W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie SIEM w ramach Pierwszej Linii Wsparcia oraz Drugiej Linii wsparcia w trybie 24/7, 7 dni w tygodniu.  Pierwsza linia (L1) wsparcia będzie odpowiedzialna za:   1. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie z warunkami SLA:  |  |  | | --- | --- | | Priorytet zdarzenia | Czas od wykrycia przez L1 do | | Podjęcia | | Poważny | 30 min | | Wysoki | 60 min | | Średni | 2 h | | Niski | 4 h |      1. Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji. 2. Analizę i rekomendację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji. 3. Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa. 4. Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji. 5. Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji. 6. Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive). 7. Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa. 8. Przygotowywanie miesięcznych raportów wykrytych zdarzeń bezpieczeństwa.     Druga linia (L2) wsparcia będzie odpowiedzialna za:   1. Dostępność usługi dla Zamawiającego zgodnie z warunkami SLA:  |  |  | | --- | --- | | Priorytet incydentu | Czas od eskalacji pierwszej linii wsparcia do L2 | | Podjęcia | | Poważny | 30 min | | Wysoki | 60 min | | Średni | 2 h | | Niski | 4 h |      1. Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych. 2. Przygotowywanie i realizację Scenariuszy użycia systemu SIEM zgodnie z wymaganiami przedstawionymi przez Zamawiającego. 3. Przygotowanie Scenariuszy Reakcji. 4. Przygotowanie Miesięcznych raportów z realizacji prac.     W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.  Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez pierwsza linię wsparcia a czasem nadania priorytetu.  Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski zgodnie z poniższym zestawieniem:  Poważny:   1. Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; 2. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego  Indicator of Compromise (pol. Wskaźnika skompromitowania); 3. Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); 4. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; 5. Informacja o potencjalnym cyberzagrożeniu  od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; 6. Potwierdzona informacja o potencjalnym cyberzagrożeniu od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; 7. Informacja o potencjalnym cyberzagrożeniu od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 8. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 9. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; 10. Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej; 11. Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego KSC lub RODO;     Wysoki   1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicators of Compromise (pol. Wskaźnika skompromitowania) na systemie chronionym; 2. Ujawnienie zestawionej sesji zwrotnej z C&C(Command & Control), trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min); 3. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej; 4. Informacja o potencjalnym cyberzagrożeniu  od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; 5. Potwierdzona Informacja o potencjalnym cyberzagrożeniu od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; 6. Informacja o potencjalnym cyberzagrożeniu  od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 7. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 8. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; 9. Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); 10. Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;     Średni   1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicators of Compromise (pol. Wskaźnika skompromitowania) na systemie chronionym; 2. Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; 3. Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; 4. Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa; 5. Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie;   Niski   1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.     Zamawiający wymaga każdorazowo po wystąpieniu Incydentu o priorytecie Poważnym i Wysokim Raportu Poincydentalnego nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:   * Unikalny identyfikator zdarzenia * Kiedy incydent wystąpił? * Kiedy incydent został zauważony / wykryty? * Jaki proces był sprawcą incydentu? * Co się wydarzyło? * Gdzie wydarzenie miało miejsce? * Dlaczego zdarzenie mogło wystąpić? * Jakie czynności powinny zostać przeprowadzone przez Zamawiającego w celu powstrzymania incydentu?     Zamawiający wymaga, aby każdy miesiąc świadczenia Usług podsumowany został Raportem Miesięcznym wg według wzoru przedstawionego przez Wykonawcę.  Wykonawca zobowiązany jest przedstawić Raport w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa. Opis incydentu powinien składać się z sekcji:   * Monitorowanie cyberbezpieczeństwa : * Data świadczenia usług * Zestawienie obsłużonych incydentów * Identyfikator incydentu * Nazwa * Klasyfikacja priorytetu Incydentu * Dokładna data i godzina ujawienia incydentu * Statusy końcowe * Ogólne rekomendacje i zalecenia dla Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.     W ramach usługi SoC Zamawiający wymaga, aby Wykonawca minimum raz w miesiącu przeprowadził spotkanie (Zamawiający dopuszcza formę zdalnego spotkania), na którym będą przedstawione oraz omówione najczęściej występujące zdarzenia wraz z propozycjami dostosowania rozwiązania SIEM celem ograniczenia występowania incydentów False Positive, czyli gdy wykryto atak lub zagrożenie, podczas gdy nie miały one miejsca. |
| **Ilość** | 1 szt. |

# Obszar kompetencyjny

## Szkolenia dla działu IT typ 1

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkoleń** |
| Typ | Szkolenie z Klastra HA |
| **Wymagania podstawowe** | Wykonawca zapewni szkolenia z obsługi i funkcjonowania dostarczonego w ramach postępowania klastra HA (składającego się z 2 serwerów opisanych w OBSZARZE TECHNICZNYM w punkcie 2. oraz macierzy opisanej w punkcie 3 niniejszego postępowania). Szkolenie dla 1 administratora, trwające min 6h.  Szkolenie w formie zdalnej. Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie do 12 miesięcy |
| **Wymagania szczegółowe** | Szkolenie musi obejmować w zakresie minimum:  Omówienie interfejsu niskopoziomowego zarządzania, w tym tworzenia grup RAID, generowania logów dla pomocy technicznej, zarządzania powiadomieniami email, korzystania w virtualnej konsoli. Omówienie skonfigurowanego serwera w tym tworzenia maszyn wirtualnych, wskazania miejsca konfiguracji sieci dla usług wirtualizatora, konfiguracji dysków twardych. Omówienie konfiguracji klastra.  Szkolenie musi obejmować zakresem konfigurację nowych volumenów, ich usuwania, przypisania do hosta lub klastra serwerów, zarządzania migawkami oraz procesu aktualizacji oprogramowania, proces generowania logów dla pomocy technicznej i procesu adresacji nowych interfejsów macierzy dla tzw. frontendu. |
| **Typ** | Szkolenie z zakresu rozwiązania typu SIEM |
| **Wymagania podstawowe** | Wykonawca zapewni szkolenie z zakresu rozwiązania typu SIEM (opisanym w OBSZARZE TECHNICZNYM w punkcie 5 niniejszego postępowania). Szkolenie dla 1 administratora, trwające min 8h.  Szkolenie w formie zdalnej. Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie do 12 miesięcy |
| **Wymagania szczegółowe** | Szkolenie ma zostać przeprowadzone dla maksymalnie 2 osób trwające minimum 1dzień roboczy.  Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie musi obejmować zakresem tworzenie reguł bezpieczeństwa, zarządzanie incydentami, dodawanie nowych źródeł logów oraz ich aktywacji. Dodatkowo musi zawierać instruktarz pozwalający na samodzielne wykonywanie aktualizacji wdrożonego produktu, jak i rozwiązywanie problemów i generowanie logów dla pomocy technicznej. |
| **Typ** | Szkolenie z UTM |
| **Wymagania podstawowe** | Wykonawca zapewni szkolenie z rozwiązania typu UTM (opisanym w OBSZARZE TECHNICZNYM w punkcie 1 niniejszego postępowania ). Szkolenie dla 1 administratora, trwające min 6h.  Szkolenie w formie zdalnej. Szkolenie zostanie dostarczone w formie vouchera, z możliwością zrealizowania w wybranym przez Administratora terminie do 12 miesięcy. |
| **Wymagania szczegółowe** | Szkolenie ma obejmować:  Rejestracja w strefie klienta i dostęp zasobów   * Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego * Ustawienia systemowe i uprawnienia administratorów * Instalacja licencji i aktualizacja systemu * Tworzenie kopii zapasowej i przywracanie konfiguracji  1. Zbieranie logów i monitorowanie    * Przedstawienie kategorii zbieranych logów    * Wykresy historyczne i monitorowanie 2. Obiekty    * Typy obiektów oraz ich wykorzystanie    * Obiekty sieciowe i obiekt typu „router” 3. Konfiguracja sieci    * Tryby pracy urządzenia    * Typy interfejsów    * Typy routingu oraz ich priorytety 4. Translacja adresów sieciowych (NAT) 5. Translacja połączeń wychodzących (maskarada) 6. Translacja połączeń przychodzących (przekierowanie) 7. Translacja dwukierunkowa (jeden do jeden) 8. Filtrowanie ruchu sieciowego (Firewall) 9. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)    * Szczegółowy opis parametrów reguły Firewall    * Kolejność przetwarzania reguł Firewall i NAT 10. Ochrona aplikacji     * Implementacja filtrowania URL dla ruchu http i https     * Konfigurowanie skanowania antywirusowego i modułu Breach Fighter     * Moduł IPS i stosowanie profili inspekcji 11. Użytkownicy i uwierzytelnianie 12. Konfiguracja usługi katalogowej     * Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)     * Rejestracja użytkowników     * Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania 13. Wirtualne sieci prywatne (VPN)     * Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)     * Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)     * Tunele VTI 14. SSL VPN     * Zasada działania     * Konfiguracja |
| **Wymagania dodatkowe** | Zamawiający wymaga, aby szkolenia dedykowane dla pracowników jednostki zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. |
| **Ilość** | 1 szt. |

## Szkolenia dla działu IT typ 2

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkoleń** |
| **Typ** | Szkolenia dla pracowników spoza działu IT |
| **Przygotowanie i przeprowadzenie kampanii phishingowej** | Zakres i planowany przebieg Testów phishingowych (TP) w zakresie minimum:   1. Zamawiający wymaga ustalenia scenariusza w zakresie minimum: Opracowania i zatwierdzenie z Zamawiającym szczegółowego scenariusza ataku socjotechnicznego. Wyboru metod i narzędzi do jego realizacji. Szczegóły kampanii, w tym scenariusze socjotechniczne oraz harmonogram realizacji, muszą zostać ustalone i zatwierdzone przez Zamawiającego co najmniej 14 dni przed planowanym rozpoczęciem kampanii. 2. Zamawiający wymaga przeprowadzenia przygotowań ataku w zakresie minimum:  * Projektowanie minimum 2 szablonów mailowych * Przygotowanie minimum 2 fałszywych domen i konfiguracja hostingu. * Listy odbiorców * Finalizacja listy docelowych odbiorców w oparciu o informacje uzyskane od Zamawiającego.  1. Zamawiający wymaga przeprowadzenie startu realizacji ataku w zakresie minimum:  * Rozpoczęcie kampanii phishingowej: * Kampania musi zostać przeprowadzona w ciągu minimum 3 dni, rozpoczynając się od wysyłki mailowej do wybranych odbiorców.  1. Zamawiający wymaga kontynuacji kampanii i monitorowania w zakresie minimum:  * Dostosowania harmonogramu wysyłki do ustaleń przeprowadzonych z Zamawiającym na etapie ustalania scenariusza. * Czas trwania kampanii od min 3 dni roboczych zostaje dostosowana w oparciu o ustalenia z Zamawiającym przeprowadzone podczas pierwszego etapu – Ustalenie scenariusza. * Kampania powinna być realizowana etapami, z wysyłkami dokonywanymi w określonych partiach i godzinach, aby zapewnić maksymalną skuteczność. * Monitorowanie reakcji * Bieżące śledzenie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami * Analiza efektywności i w razie potrzeby, wprowadzanie zmian w strategii kampanii.  1. Zamawiający wymaga przeprowadzenia zakończenia kampanii i przygotowanie raportu w zakresie minimum:  * Zakończenie wysyłki mailowej * Zebrania i dokonanie pierwszej analizy zebranych danych na temat interakcji i reakcji na przeprowadzone działania. * Przygotowania raportu końcowego dotyczącego skuteczności kampanii, zawierającego wszystkie zebrane dane, w zakresie minimum: * Opis wykorzystanych i skonfigurowanych domen * Opis szablonów oraz opis celu jaki stanowi podczas realizacji kampanii * Opis niebezpieczeństw związanych z dalszymi krokami prawdziwego ataku * Statystyki kampanii phishingowej, w tym: liczby wysłanych, otwartych maili, liczby kliknięć w link, liczby osób, które podały swoje dane. * Podsumowanie oraz rekomendacje |
| **Przeprowadzenie szkolenia** | Szkolenie musi zostać przeprowadzone w minimum 3 grupach 18-tu osobowych. Szkolenie dla każdej grupy musi trwać minimum 1 h.  Szkolenie musi obejmować w zakresie minimum:   * Wycieki informacji – mechanizmy i skutki. * Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze. * Psychomanipulacja w sieci – zasady i zastosowania. * Sfałszowane komunikaty i strony – identyfikacja zagrożeń. * Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing) * Archiwizacja internetowa – cyfrowy ślad nie znika. * Mechanizmy śledzenia w sieci – rola i funkcja cookies. * Niebezpieczeństwa ze strony nieautoryzowanego sprzętu. * Ataki siłowe na hasła – jak nie dać się złamać. * Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing). * Świadomość pracowników – kultura bezpieczeństwa w organizacji. |
| **Wymagania dodatkowe** | Zamawiający wymaga, aby szkolenia dedykowane dla pracowników jednostki zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. |
| **Ilość** | 1 szt. |