**ZP.271.2.2025 Załącznik nr 1 do SWZ**

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

|  |
| --- |
|  |

Spis treści

[Wstęp 3](#_Toc181964523)

[I. WYMAGANIA OGÓLNE 4](#_Toc181964524)

[1. RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ 4](#_Toc181964525)

[II. Obszar techniczny 6](#_Toc181964526)

[UTM Unified Threat Management 6](#_Toc181964527)

[Sprzęt serwerowy wraz z niezbędnym oprogramowaniem 13](#_Toc181964528)

[UPS, urządzenie UPS- wymagania minimalne 19](#_Toc181964529)

[Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X 20](#_Toc181964530)

[Oprogramowanie antywirusowe 21](#_Toc181964531)

[Oprogramowanie do wykonywania kopii zapasowych 26](#_Toc181964532)

[Oprogramowanie SIEM (Security Information and Event Management) 35](#_Toc181964533)

[Oprogramowanie do monitorowania infrastruktury informatycznej 58](#_Toc181964534)

[III. Obszar kompetencyjny 62](#_Toc181964535)

[Szkolenia dla działu IT typ 1 - szkolenia dotyczące oprogramowania do kopi zapasowych 62](#_Toc181964536)

[Szkolenia dla działu IT typ 2 - szkolenie dotyczące oprogramowania do monitorowania infrastruktury informatycznej 62](#_Toc181964537)

[Szkolenia dla działu IT typ 3 - szkolenie dotyczące urządzenia UTM 63](#_Toc181964538)

[Szkolenia dla pracowników spoza działu IT typ 4 - szkolenia pracowników 64](#_Toc181964539)

# Wstęp

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Pszczew 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: “ Zainstalowany jeden procesor 8-rdzeniowy, min. 2.3Ghz klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku 20.900 w teście Average CPU Mark Multithread Rating dostępnym na stronie https://www.cpubenchmark.net/ należy rozumieć jako:

“Zainstalowany co najmniej jeden procesor, posiadający co najmniej 8 rdzeni, klasy co najmniej x86, posiadające taktowanie co najmniej 2.3GHz, umożliwiające osiągnięcie wyniku co najmniej 20 900 w teście Average CPU Mark Multithread Rating dostępnym na stronie https://www.cpubenchmark.net/”.

# Obszar techniczny

## UTM Unified Threat Management

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Urządzenie UTM Unified Threat Management dla Urzędu Gminy w Pszczewie wraz z niezbędnymi serwisami i aktualizacjami. |
| **Wymagania techniczne** | Dostarczane urządzenie klasy UTM musi posiadać następujące minimalne funkcje:   1. Obsługa sieci w zakresie minimum: Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. 2. Zapora korporacyjna (Firewall) w zakresie minimum:  * Urządzenie musi być wyposażone w Firewall klasy Stateful Inspection. * Urządzenie musi obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. * Urządzenie musi dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). * Interface (GUI) do konfiguracji firewall musi umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca musi mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. * Administrator musi 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, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. * Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. * Administrator musi mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. * Edytor reguł firewall musi posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). * Firewall musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). * Urządzenie musi umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu. * System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.  1. Intrusion prevention system (IPS) w zakresie minimum:  * System detekcji i prewencji włamań (IPS) musi być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. * Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. * Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. * Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. * Moduł IPS musi nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. * Urządzenie musi mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. * Administrator urządzenia musi 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. * Urządzenie musi mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. * Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.  1. Kształtowanie pasma (Traffic Shapping) w zakresie minimum:  * Urządzenie musi mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. * Ograniczenie pasma lub priorytetyzacja musi być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. * Rozwiązanie musi umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). * Urządzenie musi umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.  1. Ochrona antywirusowa- wymagania minimalne:  * Rozwiązanie musi zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). * Co najmniej jeden z dwóch skanerów antywirusowych musi być dostarczany w ramach podstawowej licencji. * Administrator musi mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. * Administrator musi 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 musi być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.  1. Ochrona antyspam- wymagania minimalne:  * Producent musi udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). * Ochrona antyspam musi działać w oparciu o:  1. Białe/czarne listy 2. DNS RBL 3. Heurystyczny skaner 4. Wirtualne sieci prywatne (VPN)- wymagania minimalne:  * Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). * Odpowiednio kanały VPN można budować w oparciu o:  1. PPTP VPN, 2. IPSec VPN, 3. SSL VPN  * SSL VPN musi działać w trybach Tunel i Portal * W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. * Urządzenie musi posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). * Urządzenie musi posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. * Urządzenie musi umożliwiać tworzenie tuneli w oparciu o technologię Route Based.  1. Filtr dostępu do stron www- wymagania minimalne:  * Urządzenie musi posiadać wbudowany filtr URL. * Filtr URL musi działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. * Administrator musi mieć możliwość dodawania własnych kategorii URL. * Urządzenie nie może być limitowane pod względem kategorii URL dodawanych przez administratora. * Administrator musi posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:  1. Blokowanie dostępu do adresu URL, 2. Zezwolenie na dostęp do adresu URL, 3. Blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora  * Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. * Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. * Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. * Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. * Urządzenie musi posiadać możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.  1. Uwierzytelnianie- wymagania minimalne:  * Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:  1. lokalną bazę użytkowników (wewnętrzny LDAP), 2. zewnętrzną bazę użytkowników (zewnętrzny LDAP), 3. usługę katalogową Microsoft Active Directory.  * Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. * Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:  1. SSL, 2. Radius, 3. Kerberos.  * Urządzenie musi posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. * Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. * Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.  1. Administracja łączami do internetu (ISP) – wymagania minimalne:  * Urządzenie musi posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). * Mechanizm równoważenia obciążenia łącza internetowego musi działać w oparciu o następujące dwa mechanizmy:  1. Równoważenie względem adresu źródłowego, 2. Równoważenie względem połączenia.  * Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. * Urządzenie musi posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. * Urządzenie musi posiadać mechanizm statycznego trasowania pakietów. * Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu. * Urządzenie musi wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. * W zarkresie SD-WAN urządzenie musi zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów) * Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. * Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. * Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.  1. Pozostałe usługi i funkcje rozwiązania:  * Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. * Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. * Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. * Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. * Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. * Urządzenie musi posiadać usługę DNS Proxy.  1. Administracja urządzeniem- wymagania minimalne:  * Konfiguracja urządzenia musi być możliwa z wykorzystaniem polskiego interfejsu graficznego. * Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. * Komunikacja może odbywać się na porcie innym niż https (443 TCP). * Urządzenie musi być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. * Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: braku dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. * Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. * Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. * Wbudowany webowy, grafczny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. * Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. * Urządzenie musi mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). * Rozwiązanie musi mieć możliwość eksportowania logów za pomocą protokołu IPFIX. * Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. * Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. * Urządzenie musi mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów. * Zamawiająacy wymaga dostarczenia wraz z urządzeniem karty microSD o pojemności minimum 128GB o podwyższonej żywotności.  1. Raportowanie- wymagania minimalne:  * Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. * System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. * System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. * System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. * System raportujący musi dawać możliwość edycji konfiguracji z poziomu raportu. * Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenie raportów w postaci wirtualnej maszyny. * Dodatkowy system musi umożliwiać tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.  1. Parametry sprzętowe- wymagania minimalne:  * Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash. * Urządzenie musi być wyposażone w zintegrowany port na kartę microSD. * Liczba portów Ethernet 2,5Gbps- min. 8. * Liczba portów światłowodowych 1 Gbps- min. 1. * Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. * Przepustowość Firewall (1518 bajtów UDP) – min. 4Gbps * Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP)– min. 2 Gbps. * Przepustowość filtrowania Antywirusowego – min. 500 Mbps. * Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1Gbps. * Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100. * Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – min. 50 * Maksymalna liczba tuneli typu SSL VPN (tryb portalu)- min. 50 * Obsługa interfejsów 802.11q (VLAN) – min. 128. * Liczba równoczesnych sesji- minimum 300 000 i nie mniej niż 20 000 nowych sesji na sekundę. * Urządzenie ma możliwość zbudowania klastra wysokiej dostępności HA co najmniej w trybie Active-Passive. * Urządzenie nie może mieć limitu na liczbę użytkowników. * Liczba reguł filtrowania- min. 8192. * Liczba tras statycznego routingu- min. 512. * Liczba tras dynamicznego routingu- min. 10000 * Urządzenie musi umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza. |
| **Wdrożenie** | Zamawiający wymaga przeprowadzenie wdrożenia dostarczonego urządzenia UTM w zakresie minimum:   * Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu * Przeniesienie konfiguracji z obecnie posiadanego rozwiązania (Reguły firewall/NAT, konfiguracja interfejsów, routing statyczny, DHCP, IPSec VPN do 10 tuneli) * Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) * Integracja z Active Directory + Agent SSO * Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. * Uruchomienie funkcji automatycznego backupu konfiguracji. * Uruchomienie funkcji DNS proxy. * Uruchomienie wbudowanego systemu raportowania. * Uruchomienie powiadomień mailowych * Konfiguracja zbierania logów * Uruchomienie agenta SNMP * Przygotowanie Dokumentacji powdrożeniowej   Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania, który będzie potwierdzeniem posiadania umiejętności min z zakresu: (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 |
| **Gwarancja** | Urządzenie i licencja muszą być objęte gwarancją producenta w minimalnym terminie do 30.06.2026 |
| **Ilość** | 1 szt. |

## Sprzęt serwerowy wraz z niezbędnym oprogramowaniem

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Sprzęt serwerowy wraz z niezbędnym oprogramowaniem dla Urzędu Gminy w Pszczewie |
| **Obudowa** | Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3,5”. |
| **Płyta główna** | Płyta główna z możliwością instalacji fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM. Płyta główna powinna mieć możliwość zabezpieczenia pamięci ECC. |
| **Procesor** | Zainstalowany minimum jeden procesor 8-rdzeniowy, min. 2.3Ghz klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku 20.900 w teście Average CPU Mark Multithread Rating dostępnym na stronie <https://www.cpubenchmark.net/>. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim. |
| **Pamięć RAM** | Co najmniej 64 GB pamięci RAM RDIMM o częstotliwości taktowania minimum 3200MHz.  Wymaga się obsadzenie minimum 2 kości per procesor w celu zwiększenia wydajności oferowanego rozwiązania. |
| **Sloty PCI Express** | Funkcjonujące sloty PCI Express:  - minimum 2 sloty PCI Express Gen4 |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). |
| **Dyski twarde** | * Min. 4 szt. jednakowe dyski Hot-Plug SATA3 SSD o pojemności 480GB każdy, min. DWPD 3. * Min. 1 szt. dysk Hot-Plug SATA3 HDD o pojemności 2TB każdy. * Możliwość zainstalowania karty obsługującej dyski M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. * Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde oraz slotów PCIe. |
| **Kontroler RAID** | Zainstalowany sprzętowy kontroler dysków SAS/SATA z 8GB cache z podtrzymaniem oraz funkcjonalnością RAID 0,1,10,5,6,50,60. (nie dopuszcza się instalacji w wymaganych slotach PCIe) |
| **Wbudowane porty** | Minimum 5 portów USB z czego min. 2 w technologii 3.0  Minimum 1x VGA |
| **Video** | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920x1200 pikseli |
| **Napęd optyczny** | Zainstalowany w obudowie napęd DVD RW. |
| **Chłodzenie i zasilanie** | Min. 6 wentylatorów  Redundantne zasilacze o mocy minimum 700W wraz z kablami zasilającymi. |
| **System operacyjny/dodatkowe oprogramowanie** | Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Zamawiający wymaga dostarczenia min. 30 sztuk licencji dostępowych do zakupionego serwera dla urządzeń.  Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  SSO musi posiadać następujące, wbudowane cechy:   * 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,   2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,   3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,   4. 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,   5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,   6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,   7. 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),   8. Wbudowane wsparcie instalacji i pracy na wolumenach, które:      1. pozwalają na zmianę rozmiaru w czasie pracy systemu,      2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,      3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,      4. umożliwiają zdefiniowanie list kontroli dostępu (ACL),   9. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,   10. wbudowane szyfrowanie dysków   11. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,   12. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,   13. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,   14. graficzny interfejs użytkownika,   15. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,   16. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),   17. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,   18. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,   19. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:       1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC       2. 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: * podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, * ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, * odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,   + 1. zdalna dystrybucja oprogramowania na stacje robocze,     2. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,     3. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: * dystrybucję certyfikatów poprzez http, * konsolidację CA dla wielu lasów domeny, * automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, * szyfrowanie plików i folderów, * szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), * możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, * serwis udostępniania stron WWW, * wsparcie dla protokołu IP w wersji 6 (IPv6),   + 1. 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: * dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, * obsługi ramek typu jumbo frames dla maszyn wirtualnych, * obsługi 4-KB sektorów dysków, * nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, * możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, * możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  1. 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, 2. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), 3. możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, 4. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, 5. możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF |
| **Diagnostyka i bezpieczeństwo** | * Zintegrowany z płytą główną moduł TPM 2.0 * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |
| **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; * 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; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; |
| **Oprogramowanie do zarządzania** | * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * Integracja z usługą katalogową, * 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 opraciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w opraciu 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 aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * 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 zarzadzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. * Dostarczone oprogramowanie powinno umożliwiać stworzenie niestandardowego automatycznego działania dla wykrytego zdarzenia * 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. * Integracja oprogramowanie zarządzającego z konsolami zarządzania typu vCenter i MS System Center * Dostarczone oprogramowanie powinno umożliwiać zarządzanie urządzeniami firm trzecich bez potrzeby instalacji dedykowanego oprogramowania. * Umożliwia aktualizację firmware i sterowników komponentów serwera * Obsługa do minimum 8000 urządzeń per instancja |
| **Certyfikaty** | * Serwer aplikacji musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub normami równoważnymi * Serwer aplikacji musi posiadać deklarację CE lub równoważną |
| **Warunki gwarancji** | Minimum 36 miesięcy gwarancji producenta, realizowana w miejscu zgłoszenia, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta.  Uszkodzone dyski twarde pozostają u Zamawiającego.  Serwer musi spełniać wymagania normy NIST SP 800-193 lub równoważnej ochrony przed cyberatakami.  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 równoważnymi. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).Firma serwisująca musi posiadać ISO 9001:2008 lub normę równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.  Na potwierdzenie wymogu wymagane jest dołączenie do oferty oświadczenia producenta, 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.   Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. |
| **Ilość** | 1 szt. |

## UPS, urządzenie UPS- wymagania minimalne

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | UPS dla Urzędu Gminy w Pszczewie |
| **Wymagania ogólne** | Moc wyjściowa (pozorna / czynna)   * minimum 1500 VA * minimum 1000 W   Topologia: VI (line interactive)  Typ obudowy: rack  Temperatura pracy minimum: 0 ÷ +40 °C |
| **Wejście** | Napięcie znamionowe (wartość skuteczna): 230 V AC  Zakres napięcia wejściowego (wartości skuteczne): 220-240V  Częstotliwość znamionowa napięcia wejściowego: 50 Hz  Zakres częstotliwości i tolerancja: 50-60 Hz ± 3 Hz |
| **Wyjście** | Napięcie znamionowe (wartość skuteczna): 230 V AC  Zakres napięcia wyjściowego (wartości skuteczne): 220-240 V  Automatyczna regulacja napięcia (AVR)  Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej): Sinusoidalny  Częstotliwość znamionowa napięcia wyjściowego: 57-63 Hz  Czas przełączenia na pracę rezerwową (zakres) minimum: 6-10ms  Czas powrotu na pracę sieciową: minimum 0 ms |
| **Czas podtrzymania** | Czas podtrzymania z baterii wewnętrznych ( 100 % / 80 % / 50 % Pmax): minimum 7/ 10 /25 min |
| **Zabezpieczenia** | Znamionowa energia przepięcia: Nie mniejsza niż 459 J  Zabezpieczenie wejściowe: Przeciwprzepięciowe |
| **Wyposażenie i funkcje dodatkowe** | Przyłącze zasilania UPS minimum: IEC 320 C14  Przyłącza wyjściowe (liczba i typ gniazd) minimum: 4x IEC 320 C13 , 2x IEC Jumpers C13  Sygnalizacja minimum:   * Akustyczno – optyczna; wyświetlacz LED * dwukolorowe diody LED informujące o pracy bateryjnej/sieciowej, o procentowym poziomie obciążenia oraz stanie naładowania/rozładowania akumulatorów   Interfejsy komunikacyjne minimum: 1 x RS-232, 1 x USB  Oprogramowanie monitorująco-zarządzające wymagania minimalne:   * oprogramowanie do zarządzania i monitorowania pracy UPS . * wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. |
| **Certyfikaty i wymagane normy** | Minimum:   * Deklaracja CE lub normę równoważną * EN/IEC 62040-1:2019/A11:2021 lub równoważną * EN/IEC 62040-2:2006/AC:2006 lub równoważną * EN/IEC 62040-2:2018 lub równoważną |
| **Gwarancja** | Gwarancja: minimum 36 miesięcy na elektronikę i minimum 24 miesiące na akumulatory  Serwis musi być realizowany przez autoryzowany serwis producenta  Zamawiający wymaga, aby serwis realizowany był w systemie door to door |
| **Ilość** | 2 szt. |

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

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Typ** | Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X- przełącznik sieciowy da Urzędu Gminy w Pszczewie |
| **Obudowa** | Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia. |
| **Porty** | Minimum 48 portów 10/100/1000Mbps RJ45, minimum 4 porty SFP 1GbE,  Obsługa modułów SFP: 1000BASE-SX, 1000BASE-FX |
| **Wydajność przełącznika** | Minimum 16000 adresów MAC  Switch fabric capacity 104.0 Gbps  Forwarding rate min. 77 Mpps  Pamięć flash min. 256 MB  Pamięć RAM min. 512 MB |
| **Funkcjonalność warstwy II** | Przełącznik zarządzalny  Wsparcie dla technologii VLAN 802.1q  Wsparcie dla VLAN Q-in-Q  Wsparcie dla Private VLAN  Jednoczesna obsługa min. 4k VLAN  Wsparcie dla agregacji LACP (802.3ad)  Obsługa 8 grup LACP i 8 portów fizycznych per grupa  Jumbo Frames min. 9k bajtów  GVRP  GARP  UDLD |
| **Funkcjonalność warstwy III** | IPv4 routing  IPv6 routing  Obsługa dynamicznego protokołu routtingu RIP v2  Obsługa routingu bezklasowego  Policy-Based Routing (PBR)  IGMP v1, v2, v3  IGMP Querier  IGMP Proxy |
| **Inne funkcjonalności** | DHCP Server  DHCP Relay |
| **Zgodność z protokołami** | 802.1AB LLDP  802.1D Bridging, Spanning Tree  802.1p Ethernet Priority (User Provisioning and Mapping)  802.1Q VLAN Tagging, Double VLAN Tagging, GVRP  802.1W Rapid Spanning Tree (RSTP)  802.1s Multiple Spanning Tree (MSTP)  802.3 10BASE-T  802.3ab Gigabit Ethernet (1000BASE-T)  802.3ac Frame Extensions for VLAN Tagging  802.3ad Link Aggregation with LACP  802.3az Energy Efficient Ethernet (EEE)  802.3x Flow Control  802.3z Gigabit Ethernet (1000BASE-X) |
| **Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa** | 826 ARP  1155 SMIv1  1157 SNMPv1  1212 Concise MIB Definitions  1213 MIB-II  1286 Bridge MIB  1350 TFTP  2011 IP MIB  2012 TCP MIB  2013 UDP MIB  2233 Interfaces Group using SMIv2  2863 Interfaces MIB  3413 SNMP Applications  4251 SSHv2 Protocol  4252 SSHv2 Authentication  4253 SSHv2 Transport  4254 SSHv2 Connection Protocol  4293 MIB IPV6  4330 SNTP  4419 SSHv2 Transport Layer Protocol  4443 ICMP v6  4716 SECSH Public Key File Format |
| **Inne** | Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza |
| **Gwarancja** | Minimum 36 miesięcy gwarancji producenta |
| **Ilość** | 1 szt. |

## Oprogramowanie antywirusowe

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie antywirusowe dla Urzędu Gminy w Pszczewie |
| **Wymagania ogólne** | W ramach dostawy Zamawiający wymaga dostarczenia wznowienia aktualnie posiadanej licencji na oprogramowanie antywirusowe Bitdefender Gravity Zone Business Security (obejmującej 30 stanowisk) na okres do 30.06.2024r.  Zamawiający dopuszcza dostarczenie oprogramowania równoważnego (wymianę w/w oprogramowania) spełniającego poniższe wymagania minimalne.  Ponadto, w przypadku dostawy oprogramowania równoważnego Zamawiający wymaga dodatkowo:   * wdrożenia * skonfigurowania dla wszystkich użytkowników * przeszkolenia administratorów z dostarczonego oprogramowania, wg ustaleń z Zamawiającym |
| **Opis równoważności- wymagania minimalne:** | |
| **Ochrona antywirusowa i antyspyware** | 1. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona musi być dostępna w języku polskim. 3. Wykrywanie zagrożeń i analiza procesów musi przebiegać z wykorzystaniem technik heurystycznych. 4. Powiadomienia z modułu sprawdzającego procesy muszą posiadać identyfikator procesu nadrzędnego i wiersz poleceń. 5. Oprogramowanie musi wykrywać i usuwać niebezpieczne aplikacje typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 6. Oprogramowanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 7. Oprogramowanie musi posiadać funkcjonalność skanowania w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Oprogramowanie musi mieć możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików. 9. Oprogramowanie musi mieć możliwość skanowania dysków sieciowych i dysków przenośnych. 10. Oprogramowanie musi mieć możliwość skanowania plików spakowanych i skompresowanych. 11. Oprogramowanie musi mieć możliwość dodawania wykluczeni na podstawie: 12. Plik 13. Folder 14. Rozszerzenie 15. Proces 16. Hash pliku 17. Hash certyfikatu 18. Nazwa zagrożenia 19. Wiersz poleceń 20. IP/maska 21. Oprogramowanie musi posiadać możliwość skanowania i oczyszczania w czasie rzeczywistym poczty przychodzącej i wychodzącej 22. Oprogramowanie musi posiadać możliwość skanowania i oczyszczania poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego. 23. Oprogramowanie musi umożliwiać automatyczną integracje skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 24. Oprogramowanie musi posiadać możliwość skanowania ruchu http na poziomie stacji roboczych. Zainfekowany ruch musi być automatycznie blokowany i wyświetlany użytkownikowi stacji roboczej. 25. Oprogramowanie musi posiadać możliwość blokowania wybranych stron internetowych określonych przez administratora. 26. Oprogramowanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 27. Oprogramowanie musi zapewniać możliwość definiowania czy pliki z kwarantanny mają być przesłane do producenta i co jaki czas ma się ta czynność odbywać. 28. Oprogramowanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH 29. Oprogramowanie musi skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 30. Oprogramowanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 31. Oprogramowanie musi posiadać możliwość wyświetlenia danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. 32. Oprogramowanie musi posiadać możliwość wyświetlania na punkcie końcowym aktualnej wersji produktu i aktualnej wersji silników. 33. Oprogramowanie musi posiadać możliwość wyświetlania wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. 34. Oprogramowanie musi automatycznie aktualizować bazę wirusów i innych zagrożeń. 35. Oprogramowanie musi umożliwiać pobieranie aktualizacji za pośrednictwem serwera proxy. 36. Praca oprogramowania musi być niezauważalna dla użytkownika. 37. Oprogramowanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 38. Oprogramowanie musi umożliwiać stacjom roboczym łączenie się do serwera administracyjnego za pośrednictwem sieci Internet. 39. Oprogramowanie klienckie musi posiadać wbudowaną funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 40. Oprogramowanie musi posiadać możliwość odblokowania ustawień programu po wpisaniu hasła. 41. Oprogramowanie musi posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu. 42. Oprogramowanie musi posiadać budowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie). 43. Oprogramowanie musi posiadać możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. 44. Oprogramowanie musi posiadać funkcja ochrony danych która umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.). 45. Funkcja Ochrony danych może być konfigurowana zdalnie wyłącznie przez administratora. 46. Oprogramowanie musi zawierać wbudowaną zaporę osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 47. Oprogramowanie musi posiadać wbudowany IDS. 48. Oprogramowanie musi posiadać możliwość zainstalowania silnika pełnego lub lekkiego ze sprawdzaniem reputacji plików w chmurze. 49. Oprogramowanie musi posiadać możliwość tworzenia list sieci zaufanych. 50. Oprogramowanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej. 51. Oprogramowanie musi posiadać możliwość ustawienia skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 52. Oprogramowanie musi posiadać dodatkową funkcja ochrony przeciwko znanym zagrożeniom typu ransomware. 53. Oprogramowanie musi posiadać mechanizm, który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji. 54. Oprogramowanie musi zapewniać użytkownikowi na punkcie końcowym możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa). 55. Oprogramowanie musi automatycznie zezwolać na dostęp dla użytkowników Active Directory z grupy security groups. 56. Oprogramowanie musi posiadać opcję wymuszania połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. 57. Oprogramowanie musi posiadać system zarządzania ryzykiem zintegrowany z konsolą który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Ponadto, oprogramowanie musi posiadać: 58. Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:  * Ochrony przeglądarki internetowej * Sieć i poświadczenia * Błędna konfiguracja systemu operacyjnego  1. System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe. 2. System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk. 3. System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie. 4. System, który pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. 5. System, który pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach. 6. System, który pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie 7. Oprogramowanie musi posiadać wbudowaną ochronę przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również: 8. Możliwość wymuszenia funkcji DEP systemu Windows 9. Możliwość wymuszenia funkcji relokacji modułów (ASLR) 10. Oprogramowanie musi posiadać mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak: 11. Wczesny dostęp 12. Dostęp do poświadczeń 13. Wykrycie 14. Crimeware 15. Oprogramowanie musi posiadać możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. 16. Oprogramowanie musi posiadać możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. 17. Oprogramowanie musi pozwalać na odzyskanie plików minimum poniższych formatów:   3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|   1. Oprogramowanie musi dawać możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania. |
| **Stacje robocze i serwery** | 1. Oprogramowanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami na stacjach roboczych. 2. Oprogramowanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 3. Oprogramowanie musi posiadać skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”. 4. Skanowanie na żądanie musi obejmować pojedyncze pliki lub katalogi przy pomocy skrótu w menu kontekstowym. 5. Oprogramowanie musi umożliwiać skanowanie plików spakowanych i skompresowanych. 6. Oprogramowanie musi zawierać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 7. Oprogramowanie musi posiadać możliwość zablokowania hasłem odinstalowania programu. 8. Oprogramowanie i sygnatury musza być aktualizowane nie rzadziej niż raz na godzinę. 9. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 10. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych niezmienionych plików. 11. Oprogramowanie musi mieć wbudowany skaner wyszukiwania rootkitów. 12. Oprogramowanie musi mieć możliwość odblokowania ustawień po wpisaniu hasła. 13. Oprogramowanie musi mieć możliwość uruchomienia zadania skanowania z niskim priorytetem. 14. Oprogramowanie musi mieć możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego. 15. Oprogramowanie musi mieć możliwość określenia jak długo mają być przechowywane zdarzenia na stacji roboczej. 16. Oprogramowanie musi mieć możliwość zabezpieczenia hasłem klienta przed odinstalowaniem. 17. Oprogramowanie musi mieć możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym (dla systemu Linux). 18. Oprogramowanie musi mieć wbudowaną opcję automatycznego przeskanowania kwarantanny po aktualizacji sygnatur baz antywirusowych. |
| **Ilość** | 1. szt. |

## Oprogramowanie do wykonywania kopii zapasowych

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie do wykonywania kopii zapasowych |
| **Wymagania funkcjonalne dla komputerów** | 1. Oprogramowanie musi wspierać fizyczne i wirtualne komputery z systemem operacyjnym Windows oraz systemy macOS. 2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). * Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. * System musi być posiadać moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłka na wskazany adres email lub zapisywanie we wskazanym folderze) * System musi posiadać możliwość definiowania uprawnień dla administratorów systemu kopii zapasowych na poziomie dostępu do poszczególnych obiektów * System musi umożliwiać integrację z Microsoft Active Directory na poziomie zarządzania dostępem i administratorami * Oprogramowanie musi wspierać system „Single Sign On” (pojedynczego logowania ) * System musi posiadać możliwość zarządzenie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT * System musi posiadać możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją * System musi posiadać możliwość tworzenia scentralizowanych planów wykonywania kopii zapasowych * System musi posiadać możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows * System musi posiadać możliwość zdalnego uaktualniania agentów kopii zapasowych * System musi posiadać możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych * System musi posiadać możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej) * System musi posiadać możliwość zastosowania scentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych * System musi posiadać centralny katalog wszystkich danych zapisanych w kopiach zapasowych * System musi posiadać wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.  1. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Kopie zapasowe całych dysków i partycji. * Kopie zapasowe wybranych plików i folderów. * Kopia zapasowa udziałów sieciowych. * Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopii zapasowych. * Zapis kopii zapasowych na udziały sieciowe. * Zapis kopii zapasowych na serwer SFTP. * Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. * Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). * Możliwość wyszukiwania plików w kopiach zapasowych. * Możliwość szyfrowania plików kopii zapasowych. * Wsparcia dla technologii VSS. * Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. * Kompresja plików kopii zapasowych. * Możliwość replikacji kopii zapasowych na kolejne nośniki (dyski, magazyn chmurowy) * Możliwość replikacji kopii zapasowych na nośniki taśmowe * Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopii zapasowych  1. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:  * Odtworzenie całej maszyny (Windows, Mac)- tzw. Bare Metal Restore * Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. * Odtworzenie poszczególnych plików i folderów. * Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa. * Automatyzacja procesu odtwarzania całych maszyn  1. Dodatkowe wymagania związane z ochroną danych (dla poniższych funkcjonalności wymagane wsparcie dla systemu Windows 7 i nowsze):  * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. * Wbudowana ochrona antywirusowa i antymalware * Mechanizm ochrony przed exploitami. * Filtrowanie adresów URL. * Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essential. * Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji). * Mechanizm badania zdrowia dysku. * Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacji lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów , inżynierii oraz z możliwością wskazania niestandardowej aplikacji. * Filtrowanie stron na podstawie kategorii stron. * Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu, który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS. * Możliwość skanowania plików backupu w poszukiwaniu malware'u. * Bezpieczne odtwarzanie backupu - w trakcie odtwarzania backupu będzie wykonywane skanowanie w poszukiwaniu zagrożeń i ich usunięcie.  1. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:  * W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. * W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu * Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski. * Producent powinien przechowywać dane osobowe (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256. * Producent nie powinien wykorzystywać danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych. * Producent oprogramowania powinien przeprowadzać okresowe oceny ryzyka i przeglądy co najmniej raz w roku. * Infrastruktura (chmurowy magazyn kopii zapasowych) powinna być zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1). * Producent oprogramowania powinien być zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2 lub standardami równoważnymi, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie lub certyfikacjami równoważnymi. * Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania. |
| **Wymagania funkcjonalne dla serwerów** | 1. Oprogramowanie musi Wspierać systemy operacyjne: Windows Server 2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). * Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. * System musi być posiadać moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłka na wskazany adres email lub zapisywanie we wskazanym folderze) * System musi posiadać możliwość definiowania uprawnień dla administratorów systemu kopii zapasowych na poziomie dostępu do poszczególnych obiektów * System musi umożliwiać integrację z Microsoft Active Directory na poziomie zarządzania dostępem i administratorami * Oprogramowanie musi wspierać system „Single Sign On” (pojedynczego logowania) * System musi posiadać zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. * System musi posiadać możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). * System musi posiadać możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. * System musi posiadać możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows. * System musi posiadać możliwość zdalnego uaktualniania agentów kopi zapasowych. * System musi posiadać możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych. * System musi posiadać możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej). * System musi posiadać możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych. * System musi posiadać centralny katalog wszystkich danych zapisanych w kopiach zapasowych. * System musi posiadać wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego. * Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: * Kopie zapasowe całych dysków i partycji. * Kopie zapasowe wybranych plików i folderów. * Kopia zapasowa udziałów sieciowych * Kopie zapasowe aplikacji * Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. * Zapis kopii zapasowych na udziały sieciowe. * Zapis kopii zapasowych na serwer SFTP. * Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której * Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). * Możliwość wyszukiwania plików w kopiach zapasowych. * Możliwość szyfrowania plików kopii zapasowych. * Wsparcia dla technologii VSS. * Deduplikacjia kopii zapasowych na poziomie bloków danych. * Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. * Kompresja plików kopi zapasowych. * Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy). * Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją kopii zapasowych.  1. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:  * Odtworzenie całej maszyny (Windows, Mac)- tzw. Bare Metal Restore * Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. * Odtworzenie poszczególnych plików i folderów. * Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa. * Automatyzacja procesu odtwarzania całych maszyn. * Wyszukiwanie i podgląd odtwarzanych wiadomości email * Możliwość granularnego odtwarzania witryn i plików Microsoft SharePoint. * Odtwarzanie kontrolerów domeny Microsoft Active Directory.  1. Dodatkowe wymagania związane z ochroną danych dostępne dla systemów Windows Server  * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. * Wbudowana ochrona antywirusowa i antymalware. * Mechanizm ochrony przed exploitami. * Filtrowanie adresów URL. * Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essentials. * Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji). * Mechanizm badania zdrowia dysku. * Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacjach lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów, inżynierii oraz z możliwością wskazania niestandardowej aplikacji. * Filtrowanie stron na podstawie kategorii stron. * Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono oprogramowanie, stopień ważności w skali CVSS. * Możliwość skanowania plików backupu w poszukiwaniu malware’u. * Bezpieczne odtwarzanie backupu – w trakcie odtwarzania backupu będzie wykonywane skanowanie w poszukiwaniu zagrożeń i ich usunięcie.  1. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:  * W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. * W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu * Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski. * Producent powinien przechowywać dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256. * Producent nie powinien wykorzystywać danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych. * Producent oprogramowania powinien przeprowadzać okresowe oceny ryzyka i przeglądy co najmniej raz w roku. * Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1). * Producent oprogramowania powinien być zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2 lub standardami równoważnymi, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS lub równoważnymi na minimum 4 poziomie lub certyfikatami równoważnymi. * Przestrzeń chmurowa dostarczana wraz z oprogramowaniem powinna posiadać minimum 250GB w ramach jednej licencji, na cały okres jej trwania. |
| **Wymagania funkcjonalne dla środowisk wirtualizacyjnych** | 1. Oprogramowanie musi wspierać systemy operacyjne:  * Dla Hosta: Vmware, , Microsoft Hyper-V, * Dla maszyn wirtualnych:Windows Server  1. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). * Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. * System musi być posiadać moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłka na wskazany adres email lub zapisywanie we wskazanym folderze) * System musi posiadać możliwość definiowania uprawnień dla administratorów systemu kopii zapasowych na poziomie dostępu do poszczególnych obiektów * System musi umożliwiać integrację z Microsoft Active Directory na poziomie zarządzania dostępem i administratorami * Oprogramowanie musi wspierać system „Single Sign On” (pojedynczego logowania ) * System musi posiadać możliwość zarządzenie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT * System musi posiadać możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją * System musi posiadać możliwość tworzenia scentralizowanych planów wykonywania kopii zapasowych * System musi posiadać możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows * System musi posiadać możliwość zdalnego uaktualniania agentów kopii zapasowych * System musi posiadać możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych * System musi posiadać możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej) * System musi posiadać możliwość zastosowania scentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych * System musi posiadać centralny katalog wszystkich danych zapisanych w kopiach zapasowych * System musi posiadać wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.  1. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Kopie zapasowe całych dysków i partycji. * Kopie zapasowe wybranych plików i folderów. * Kopia zapasowa udziałów sieciowych. * Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi) * Kopie zapasowe aplikacji * Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopii zapasowych. * Zapis kopii zapasowych na udziały sieciowe. * Zapis kopii zapasowych na serwer SFTP. * Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. * Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery). * Możliwość wyszukiwania plików w kopiach zapasowych. * Szyfrowanie plików kopii zapasowych. * Wsparcie dla technologii VSS. * Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. * Kompresja plików zapasowych. * Replikacja kopii zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy). * Możliwość zaplanowania zadań związanych z weryfikacją, replikacją i retencją plików kopii zapasowych.  1. Oprogramowanie musi umożliwiać odtworzenie kopii zapasowych w oparciu o co najmniej:  * Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore * Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. * Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej. * Odtworzenie poszczególnych plików i folderów. * Automatyzacja procesu odtwarzania całych maszyn. * Wyszukiwanie i podgląd odtwarzanych wiadomości email. * Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.  1. Dodatkowe wymagania związane ochroną danych na systemach wewnątrz wirtualizatora (dla poniższych funkcjonalności wymagane wsparcie minimum Windows 7 i nowsze oraz Windows Server 2008 R2 i nowsze):  * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. * Wbudowana ochrona antywirusowa i antymalware. * Mechanizm ochrony przed exploitami. * Filtrowanie adresów URL. * Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essentials. * Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in. instalacja poprawki, wykonanie skanowania stacji). * Mechanizm badania zdrowia dysku. * Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacji lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów, inżynierii oraz z możliwością wskazania niestandardowej aplikacji. * Filtrowanie stron na podstawie kategorii stron. * Możliwość skanowania plików backupu w poszukiwaniu malware’u. * Bezpieczne odtwarzanie backupu- w trakcie odtwarzania backupu będzie wykonywane skanowanie w poszukiwaniu zagrożeń i ich usunięcie. * Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.  1. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:  * W przypadku uzyskania uzsadanionej pewności że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki musi dostarczyć informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. * W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby   udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu.   * Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich   repliki muszą być przechowywane na terenie Polski.   * Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie   zapasowe) przy użyciu technik szyfrowania, minimum AES-256.   * Producent nie może wykorzystywać danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych. * Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku. * Infrastruktura (chmurowy magazyn kopii zapasowych) musi być zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1). * Producent oprogramowania musi być zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2 lub standardami równoważnymi, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie lub certyfikatami równoważnymi. * Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania. |
| **Wymagania dodatkowe** | Interfejs, instrukcja i pomoc techniczna powinna być w języku polskim |
| **Licencja** | Zamawiający wymaga dostarczenia licencji w formie subskrypcji.  Licencja musi być obowiązywać do 30.06.2026r. na:   * Minimum 30 komputerów * Minimum 1 serwera * Minimum 1 maszyny wirtualnej |
| **Ilość** | 1. szt. |

## Oprogramowanie SIEM (Security Information and Event Management)

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie SIEM Security Information and Event Management dla UG |
| **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 50 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.  142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.  143. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.  144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x). |
| **Wymagania dotyczące licencji i wsparcia** | Dostarczone rozwiązanie musi być w formie licencji wieczystej oraz być objęte wsparciem producenta lub producentów minimum do 30.06.2024 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. |
| **Wdrożenie** | 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 30 źródeł logów pochodzących z minimum: serwery fizyczne, serwery wirtualne, urządzenia sieciowe, rozwiązania endpoint protection, systemów backupu. Wymaga się, aby Wykonawca przygotował harmonogram wdrożenia uwzględniający 6 etapów wdrożenia.   * 1etap - Analiza przedwdrożeniowa, * 2 etap - Instalacja systemu, * 3 etap - konfiguracja systemu, * 4 etap - dostrojenie systemu, * 5 etap - szkolenia, * 6 etap - dokumentacja powdrożeniowa.   W ramach etapu 1 wymaga się przygotowania przeprowadzenia analizy zmierzającej do określenia istotnych informacji które SIEM powinien wykrywać z podłączonych źródeł logów w ramach swojego monitoringu. Analiza ma na celu przygotowanie do stworzenia dedykowanych reguł bezpieczeństwa i ich implementacji na etapie konfiguracji systemu. W ramach etapu 2 Wykonawca musi zainstalować zaoferowane oprogramowanie według wcześniej przedstawionej architektury działania rozwiązania oraz wcześniej przygotowanego schematu komunikacji sieciowej w sieci lokalnej Zamawiającego.  W ramach etapu 3 Wykonawca musi zaimplementować wcześniej opracowanie reguły bezpieczeństwa wraz z weryfikacją ich działania dla konkretnych procesów określonych na etapie analizy przedwdrożeniowej.  W ramach etapu 4 Wykonawca wykona dostrojenie systemu 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.  W ramach etapu 5 wymagane jest przeprowadzenie szkolenia zawierającego elementy codziennej obsługi zdarzeń, ich analizy. A także sposobu dodawania nowych źródeł logów, aktualizacji systemu do nowszej wersji.  W ramach etapu 6 należy dostarczyć dokumentację powdrożeniową wskazującą wszystkie istotne elementy z punktu widzenia wdrożenia, wraz ze wszystkimi danymi dostępowymi do kont technicznych stworzonych na etapie wdrożenia. |
| **Ilość** | 1 szt. |

## Oprogramowanie do monitorowania infrastruktury informatycznej

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla oprogramowania** |
| **Typ** | Oprogramowanie do monitorowania infrastruktury informatycznej dla Urzędu Gminy w Pszczewie |
| **Monitorowanie infrastruktury** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:   1. Wykrywanie urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). 2. Wizualizacja stanu urządzeń w postaci ikon urządzeń na mapach sieci. 3. Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. 4. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Program powinien monitorować czas ich odpowiedzi i procent utraconych pakietów. 5. Serwerów pocztowych:  * program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, * program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, * program powinien mieć możliwość wykonywania operacji testowych, * program powinien mieć możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.  1. Monitorowanie serwerów WWW i adresów URL. 2. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail. 3. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 (przełączniki, routery, drukarki sieciowe, urządzenia VoIP). 4. Obsługa komunikatów syslog i pułapek SNMP. 5. Monitoring routerów i przełączników wg:  * zmian stanu interfejsów sieciowych, * ruchu sieciowego, * podłączonych stacji roboczych, * ruchu generowanego przez podłączone stacje robocze.  1. Wydajności systemów z rodziny Windows posiadanych przez Zamawiającego:  * obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. |
| **Inwentaryzacja sprzętu i oprogramowania** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:   1. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart 2. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 3. Informacja o zainstalowanych aplikacjach oraz aktualizacjach co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 4. Zbieranie informacji w zakresie zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP 5. Posiadanie możliwości wysyłania powiadomienia e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 6. Możliwość odczytania numeru seryjnego (klucze licencyjne). 7. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 8. Możliwość przeglądu informacji o konfiguracji systemu, tj. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań. |
| **Zdalna pomoc** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:   1. W ramach kontroli stacji użytkownika dostępny powinien być podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. 2. Pobieranie listy użytkowników z usługi katalogowej, 3. Przypisywanie pracowników helpdesk do kategorii zgłoszeń. 4. Procesowanie zgłoszeń użytkowników z wiadomości e-mail. 5. Dołączanie załączników do zgłoszeń. 6. Zrzuty ekranowe (podgląd pulpitu). 7. Dystrybucję oprogramowania przez Agentów. 8. Dystrybucję oraz uruchamianie plików za pomocą Agentów. 9. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku. 10. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń. 11. Planowanie nieobecności pracowników helpdesk. 12. Obsługę umów o gwarantowanym poziomie świadczenia usług (SLA). 13. Generowanie raportów obsługi helpdesk. 14. Zdalne wykonywanie poleceń poprzez Agentów (utworzenie / edycja konta lokalnego użytkownika systemu). 15. Możliwość użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. 16. Oprogramowanie powinno posiadać komunikator. 17. Oprogramowanie powinno posiadać bazę zgłoszeń umożliwiającą użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. |
| **Monitorowanie aktywności użytkowników** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:   1. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach. 2. Monitorowanie rzeczywistego użytkowania programów (procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność. 3. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt). 4. Monitorowania transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika). 5. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen. Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. 6. Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu. 7. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. 8. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. 9. Wyświetlanie statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 10. Wyświetlanie statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. 11. Grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 13. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 14. Przypisywanie kategorii aplikacjom i stronom internetowym, możliwość stworzenia predefiniowanej listy kategorii z możliwością edycji. 15. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji. |
| **Ochrona danych przed wyciekiem** | Dostarczone oprogramowanie powinno spełniać minimalne wymagania:   1. Zarządzanie prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 4. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 5. Autoryzowanie urządzeń firmowych: pendrive’ów, dysków zewnętrznych - urządzenia nieautoryzowane. 6. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 7. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 8. Możliwość usuwania z listy znanych urządzeń tych nośników. |
| **Licencja** | Licencja wieczysta na co najmniej 30 stacji roboczych. Wsparcie serwisowe producenta musi obowiązywać do 30.06.2024 r. |
| **Ilość** | * 1. szt. |

# Obszar kompetencyjny

## Szkolenia dla działu IT typ 1 - szkolenia dotyczące oprogramowania do kopi zapasowych

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla pracowników działu IT typ 1 |
| **Szkolenie z zakresu oprogramowania do wykonywania kopii zapasowych – wymagania minimalne** | Zamawiający wymaga przeprowadzenia szkolenia z systemu wykonywania kopii zapasowych, minimum jednodniowego (1), w formie zdalnej, przez certyfikowanego trenera wdrażanego rozwiązania w ramach grantu, wyspecyfikowanego w I Obszar techniczny pkt 6 Oprogramowanie do wykonywania kopii zapasowych.  Minimalny zakres tematyczny:   * Możliwości i zastosowanie produktu, * Omówienie konsoli i dostępnych możliwości, * Metody wdrożenia i automatyzacji, * Sposoby aktualizacji, * Ćwiczenia praktyczne z wdrażania systemu, * Typy chronionych danych/zasobów/usług, * Tworzenie planu backupu całego systemu oraz baz SQL, * Lokalizacje przechowywania kopii zapasowych, * Weryfikacja kopii zapasowej, * Usuwanie planu kopii zapasowej, * Dodatkowe ustawienia, * Ćwiczenia praktycznie z tworzenia planu backupu, * Metody odtwarzania kopii zapasowych, * Tworzenie i zastosowanie nośnika startowego, * Ćwiczenie praktycznie z odzyskiwania kopii zapasowych, * Administracja kontami i uprawnieniami oprogramowania. |
| **Wymagania dodatkowe** | Dodatkowo Zamawiający wymaga, aby uczestnik każdego szkolenia otrzymał:   * Materiały szkoleniowe w wersji elektronicznej * Wsparcie poszkoleniowe trenera w okresie minimum 14 dni po zakończeniu szkolenia. * Certyfikat ukończenia szkolenia * Szkolenie powinno zostać dostarczone w formie vouchera z możliwością zrealizowana w okresie 12 miesięcy od momentu dostarczenia. |
| **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 - szkolenie dotyczące oprogramowania do monitorowania infrastruktury informatycznej

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla pracowników działu IT typ 2 |
| **Szkolenie zakresu zarządzania i administracji oprogramowaniem do monitorowania infrastruktury Informatycznej – wymagania minimalne** | Zamawiający wymaga przeprowadzenia szkolenia minimum dwudniowego (2), w formie stacjonarnej w miejscu wskazanym przez producenta oprogramowania. (Wykonawca zobowiązany jest do zapewniania minimum jednego (1) noclegu dla uczestnika szkolenia), przez certyfikowanego trenera wdrażanego rozwiązania w ramach grantu, wyspecyfikowanego w I Obszar techniczny pkt 8 Oprogramowanie do monitorowania infrastruktury informatycznej.  Minimalny zakres tematyczny:   * Najważniejsze funkcjonalności oprogramowania, * Poprawna konfiguracja oprogramowania, * Wymagania i instalacja systemu, * Sposoby aktualizacji, * Ćwiczenia praktyczne z wdrażania systemu, * Monitoring krytycznych urządzeń w organizacji, * Przeprowadzanie audytu oprogramowania i sprzętu, * Monitorowanie aktywności użytkowników, * Automatyzacja procesów obsługi zgłoszeń serwisowych, * Zarządzanie nośnikami zewnętrznymi, * Zarządzanie wskaźnikami aktywności pracowników. |
| **Wymagania dodatkowe** | Dodatkowo Zamawiający wymaga, aby uczestnik każdego szkolenia otrzymał:   * Materiały szkoleniowe w wersji elektronicznej * Wsparcie poszkoleniowe trenera w okresie minimum 14 dni po zakończeniu szkolenia. * Certyfikat ukończenia szkolenia |
| **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 3 - szkolenie dotyczące urządzenia UTM

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenia dla pracowników działu IT typ 3 |
| **Szkolenie z zakresu urządzeń UTM Unified Threat Management – wymagania minimalne** | Zamawiający wymaga przeprowadzenia zaawansowanego szkolenia z urządzenia klasy UTM, minimum trzydniowego (3), w formie zdalnej, przez certyfikowanego trenera wdrażanego rozwiązania w ramach grantu, wyspecyfikowanego w I Obszar techniczny pkt 1 UTM Unified Threat Management.  Minimalny zakres tematyczny:   * Zaawansowana konfiguracja oferowanego rozwiązania. * Konfiguracja systemu IPS oraz tuneli VPN w oparciu o certyfikaty * Administracja urządzeniami w klastrach HA oraz zarządzanie certyfikatami. * Infrastruktura klucza publicznego * Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników * Zasada działania oraz zaawansowana konfiguracja SSL Proxy * Transparentne uwierzytelnianie użytkowników * Typy szyfrowania |
| **Wymagania dodatkowe** | Dodatkowo Zamawiający wymaga, aby uczestnik każdego szkolenia otrzymał:   * Materiały szkoleniowe w wersji elektronicznej * Wsparcie poszkoleniowe trenera w okresie minimum 14 dni po zakończeniu szkolenia. * Certyfikat ukończenia szkolenia * Szkolenie powinno zostać dostarczone w formie vouchera z możliwością zrealizowana w okresie 12 miesięcy od momentu dostarczenia. |
| **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 pracowników spoza działu IT typ 4 - szkolenia pracowników

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla szkolenia** |
| **Typ** | Szkolenie dla pracowników spoza działu IT  (cyberbezpieczeństwo) |
| **Szkolenie socjotechniczne phishing** | W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do przeprowadzenia testów phishingowych (TP) wg poniższego zakresu minimalnego:   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 jednego (1) szablonu mailowych * Przygotowanie minimum jednej (1) fałszywej domeny 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 minimum 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 pracowników urzędu * Bieżącego śledzenie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami * Analizy 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 - przedstawienie efektów * 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. |
| **Szkolenie z cyberbezpieczeństwa** | Szkolenie musi zostać przeprowadzone w maksymalnie 1 grupie minimum 20 osobowej. 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** | Szkolenie powinno zostać dostarczone w formie vouchera z możliwością zrealizowana w okresie 12 miesięcy od momentu dostarczenia. |
| **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. |