**ZPU.272.30.2024.** Załącznik nr 9 do SWZ

(wymagany wraz z ofertą)

# OPIS PRZEDMIOTU ZAMÓWIENIA / OPIS OFEROWANEGO SPRZĘTU

Niniejszy Załącznik stanowi jednocześnie szczegółowy opis przedmiotu zamówienia i opis oferowanego sprzętu. Zaoferowane przez Wykonawcę urządzenie musi spełniać wymagania postawione w niniejszym załączniku w kolumnie „Wymagania minimalne” oraz zostać dostarczone na warunkach określonych w SWZ.

**Wykonawca w kolumnie „Oferowane parametry” winien odnieść się do każdego z wymagań minimalnych postawionych przez Zamawiającego w kolumnie „Wymagania minimalne”. Wykonawca określa też model i producenta.**

# Tabela 1 - Przełącznik TYP I - 2 SZTUKI

|  |  |
| --- | --- |
| **PRODUCENT** |  |
| **MODEL** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **PRZEŁĄCZNIK TYP I** | | | |
| **LP** | **Parametr** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | **Porty** | Przełącznik 2U wyposażony w porty:  - 96x 25 Gigabit Ethernet SFP28  - 8x 100 Gigabit Ethernet QSFP28  - 1 port konsolowy RJ45  - 1 port zarządzający typu out-of-band management  - 1 port typu USB |  |
|  | **Kable/wkładki** | 3x kabel QSFP28/QSFP28, 100GbE, Active Optical (Optic included) Cable min. 10m  24x kabel DAC SFP+/SFP+, 10GbE, min. 5m  24x wkładka SFP+, 10GbE, SR, 850nm, 300m  24x wkładka SFP+ 10GbE BaseT, 30m, |  |
|  | **System operacyjny** | Modularny system operacyjny,  Musi być zgodny ze standardem ONIE i umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności. |  |
|  | **Zasilanie** | 2 redundantne zasilacze AC |  |
|  | **RACK** | Musi zapewniać instalację w szafach 19” |  |
|  | **Pamięć** | Pamięć CPU: 16GB  Pojemność bufora pakietów: 32MB |  |
|  | **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 3.2 Tbps (6.4 Tbps full-duplex) |  |
|  | **Chłodzenie** | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne).  Musi być wyposażone w redundantne i wymienne w trakcie pracy (hot-swappable) wiatraki |  |
|  | **Funkcjonalności warstwy II** | Musi obsługiwać ramki „Jumbo” o długości min. 9000B.  Musi obsługiwać, co najmniej 4000 VLANów.  Pamięć, dla co najmniej 128 000 adresów MAC.  Musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+, MSTP  Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy  - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń  Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG |  |
|  | **Funkcjonalności warstwy III** | Musi obsługiwać protokoły dynamicznego routingu dla IPv4 i dla IPv6: OSPF, BGP  Musi obsługiwać protokół BFD, przynajmniej dla protokołu OSPF i OSFP v3 i tras statycznych  Musi przechowywać sprzętowo minimum 32000 wpisów routingu IPv4 i 16000 wpisów routingu IPv6  Musi wspierać mechanizm L3 ECMP Load Balancing  Musi wspierać protokół redundancji VRRP  Wsparcie dla DHCP server i DHCP Relay oraz DHCPv6 Relay  Obsługa Policy Based Routing  Obsługa Muticastów, IGMP Snooping oraz Multicast Snooping, protokołu PIM oraz filtrów dla PIM  Musi obsługiwać funkcjonalność VxLAN, Static VxLan  Musi obsługiwać funkcjonalność VXLAN BGP EVPN (Ethernet VPN) z MP-BGP  Obsługa routingu między VxLAN-ami (VxLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway  Obsługa Multi-AS dla EVPN oraz trybów Asymmetric IRB (Integrated routing and bridging) oraz Symmetric IRB  Obsługa mechanizmu BGP unnumbered dla EVPN |  |
|  | **Mechanizmy bezpieczeństwa i QoS** | Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, vlan, wartość DSCP  Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi.  Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).  Implementacja mechanizmu Weighted Random Early Detection (WRED)  Obsługa IP Precedence i DSCP  Obsługa Control-Plane-Policing (ochrona systemu operacyjnego przed atakami DoS)  Musi obsługiwać DCB (Data Center Bridging)  Co najmniej 3 poziomy dostępu administracyjnego przez konsole:  Autoryzacja użytkowników/portów w oparciu o 802.1x  Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6  Obsługa protokołu Precision Time Protocol (PTP, IEEE 1588v2)  Filtrowanie dostępu do zarządzania poprzez profile dostępowe  Listy ACL sterowane czasowo  dynamiczna inspekcja ARP  minimalnie 2000 list kontroli dostępu (ACL) Do 700. reguł na listę ACL. |  |
|  | **Mechanizmy zarządzania** | Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2  Obsługa monitorowania ruchu na porcie (Port Monitoring), ACL-Based Monitoring oraz RSPAN  Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony typu ethernet 100/1000BaseT  Plik konfiguracyjny urządzenia musi być możliwy do edycji ‘off-line’. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian.  Wsparcie dla mechanizmu Beacon LED control – włączenie diody danego interfejsu celem identyfikacji  Urządzenie musi posiadać funkcjonalność automatycznej instalacji oprogramowania poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware), w trakcie pierwszego podłączenia do sieci Ethernet  Urządzenie musi mieć możliwość utworzenia skryptów systemu linux oraz uruchomienia skryptów utworzonych w języku Python oraz umożliwiać jego konfigurację przez narzędzia Ansible, Chef i Puppet  Możliwość użycia Restconf API, autoryzacja w oparciu o tokeny dla REST API oraz wsparcie dla mechanizmu tłumaczenia dowolnej komendy CLI na wywołanie Restconf |  |
|  | **Inne** | Możliwość instalacji zewnętrznych pakietów Docker-CE I uruchamiania ich w ramach systemu operacyjnego |  |
|  | **Gwarancja** | * min.5-letnia gwarancja producenta. * Usługi gwarancyjne muszą być świadczone na miejscu w siedzibie Zamawiającego, * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Czas reakcji serwisu - do końca następnego dnia roboczego. * Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych (dokumenty potwierdzające należy załączyć do oferty.) * Firma serwisująca musi posiadać ISO-27001 na świadczenie usług serwisowych (dokumenty potwierdzające należy załączyć do oferty.) * Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, * Jeżeli naprawa sprzętu nie zostanie zrealizowana w terminie do 5 dni to Wykonawca zobowiązuje się do dostarczenia sprzętu zastępczego o nie gorszych parametrach.   Dokumenty należy przedłożyć w języku polskim. Dokumenty w języku obcym powinny być złożone wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę. |  |
|  | **Dodatkowe usługi zakres prac związanych z montażem, instalacją** | Zamawiający wymaga:   1. Przeprowadzenia przez Wykonawcę audytu istniejącego przełącznika rdzenia sieci Zamawiającego pod kątem dobrych praktyk i poprawności pracy. 2. Opracowania przez Wykonawcę na podstawie wyników audytu i w konsultacji z Zamawiającym projektu technicznego wdrożenia, obejmującego między innymi:    1. Instalację dostarczonych przełączników TYP I,    2. Konfigurację mechanizmów wysokiej dostępności (klaster urządzeń).    3. Konfigurację funkcjonalności L2: VLAN, Spanning Tree, agregacji łączy (wraz z mechanizmami bezpieczeństwa),    4. Konfigurację funkcjonalności L3/L4: routing IP (statyczny/dynamiczny), listy kontroli dostępu.    5. Konfigurację zarządzania (SSH, HTTPS, SNMP).    6. Konfigurację logowania zdarzeń.    7. Opracowanie scenariuszy testów akceptacyjnych. 3. Wdrożenia przełączników TYP I zgodnie z opracowanym projektem technicznym. 4. Realizacji testów akceptacyjnych. |  |

# Tabela 2 - Przełącznik TYP II - 14 SZTUK

|  |  |
| --- | --- |
| **PRODUCENT** |  |
| **MODEL** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **PRZEŁĄCZNIK TYP II** | | | |
| **LP** | **Parametr** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | **Porty** | Minimum 48 portów gigabitowych w standardzie 100/1000BaseT  Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). |  |
|  | **Wkładki** | Przełącznik musi być wyposażony w:  - 4x wkładka SFP+, 10GbE, SR, 850nm, 300m |  |
|  | **Wymiary** | Wysokość w szafie 19” – 1U, głębokość nie większa niż 30 cm |  |
|  | **Pobór mocy** | nie większy niż 190W |  |
|  | **Przepustowość** | minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) |  |
|  | **Wydajność** | minimum 112 Mp/s |  |
|  | **Tablica adresów MAC** | Tablica adresów MAC o wielkości minimum 32000 pozycji |  |
|  | **Routing IPv4** | minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) |  |
|  | **Routing IPv6** | minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) |  |
|  | **Wielkość sprzętowej tablicy routingu** | minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6 |  |
|  | **Obsługa VxLAN** | TAK |  |
|  | **Obsługa** | Obsługa ruchu Multicast IGMP Snooping; MLD Snooping  Obsługa ramek Jumbo  Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol  Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN  Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI  Obsługa standardu 802.1p – min. 8 kolejek na porcie  Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)  Obsługa Syslog  Obsługa NTP lub SNTPv4  Obsługa protokołu VTP lub MVRP  Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego |  |
|  | **Funkcje** | Funkcja Root Guard oraz BPDU protection  Funkcja mirroringu portów  Funkcja autoryzacji użytkowników zgodna z 802.1x  Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ |  |
|  | **Funkcja łączenia w stos** | Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania.  Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie. |  |
|  | **Wsparcie** | Wsparcie dla funkcji DHCP server, DHCP Relay  Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3  Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az  Wsparcie dla funkcji Private VLAN lub równoważnego |  |
|  | **RADIUS Accounting** | TAK |  |
|  | **Protokół OpenFlow** | OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.  Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)  Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.  Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow. |  |
|  | **Zarządzanie** | Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https |  |
|  | **Inne** | Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku  Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej |  |
|  | **Dodatkowe wymagania** | Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania.  Wszystkie wymagane na przełączniku funkcje (o ile nie wyspecyfikowano inaczej) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć.  Producent sprzętu musi być sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” i znajdować się w kwadracie liderów (Leaders). |  |
|  | **Gwarancja** | Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę w trybie „best effort” – rozumiane jako wysyłka w następnym dniu roboczym z zastrzeżeniem niewystąpienia nieprzewidzianych opóźnień. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. |  |
|  | **Dodatkowe usługi zakres prac związanych z montażem, instalacją** | Zamawiający wymaga:   1. Opracowania przez Wykonawcę w konsultacji z Zamawiającym projektu technicznego wdrożenia, obejmującego między innymi:    1. Instalację dostarczonych przełączników TYP II,    2. Konfigurację funkcjonalności L2: VLAN, Spanning Tree, agregacji łączy (wraz z mechanizmami bezpieczeństwa),    3. Konfigurację zarządzania (SSH, HTTPS, SNMP).    4. Konfigurację logowania zdarzeń.    5. Opracowanie scenariuszy testów akceptacyjnych. 2. Wdrożenia przełączników TYP II zgodnie z opracowanym projektem technicznym. 3. Realizacji testów akceptacyjnych. |  |

# Tabela 3 - System NAC - 1 SZTUKA

|  |  |
| --- | --- |
| **PRODUCENT** |  |
| **MODEL** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **SYSTEM NAC** | | | |
| **LP** | **Parametr** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | **Podstawowa funkcjonalność systemu NAC** | 1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. 2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor) 3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. 4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. 5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. 6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. 7. System musi umożliwiać obsługę co najmniej 500 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 5000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. 8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego. 9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. 10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:     * VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x     * Maszyny fizyczne - serwery wspierane przez producenta. 11. System musi posiadać funkcjonalność serwerów:     * serwera RADIUS dla infrastruktury sieciowej,     * serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,     * serwera SYSLOG,     * serwera TACACS+,     * serwera Monitoringu,     * serwera DHCP,     * serwera polityk uwierzytelniania i kontroli dostępu 802.1X,     * serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. 12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. 13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. 14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. 15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now. 16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. 17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. 18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. 19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. 20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie. 21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status). 22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania. 23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). 24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci. 25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. 26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia. 27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. 28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP. 29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu. 30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. 31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. 32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci. 33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. 34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+. 35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. 36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD). 37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn. 38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS. 39. System musi posiadać funkcję personalizacji strony gościnnej. 40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon. 41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor. 42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS. 43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory. 44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory. 45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu. 46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru. 47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). 48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP. 49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni. 50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. 51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. 52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego. 53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. 54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. 55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych. 56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. 57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc). 58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA. 59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:     * Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności     * Czy włączony jest firewall     * Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur     * Czy jest włączone szyfrowanie dysku systemowego     * Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory     * Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora     * Czy w systemie są uruchomione procesy wskazane przez administratora     * Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności     * Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:       + Wartości klucza rejestru       + Typu wartości: Number, String, Version 60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. 61. System musi współpracować z serwerem tokenów. 62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:     * Microsoft Windows     * Mac OS     * iOS     * Android 63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). 64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory. |  |
|  | **Mechanizmy uwierzytelniania** | 1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. 2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:    * MAC,    * PAP/ASCII,    * CHAP,    * SNMP,    * 802.1X. 3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp. 4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. 5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. 6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). 7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:    * Tożsamość/Urządzenie końcowe,    * Grupa tożsamości/urządzeń końcowych,    * Parametry urządzeń końcowych, min: system operacyjny, wersja,    * Atrybuty Active Directory,    * Jednostka organizacyjna tożsamości/urządzeń końcowych,    * Urządzenia sieciowe sieci przewodowej, bezprzewodowej,    * Grupy urządzeń sieciowych,    * Porty urządzeń sieciowych,    * Grupy portów urządzeń sieciowych,    * Jednostka organizacyjna portów,    * Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),    * Data, czas ważności polityki,    * Wewnętrzny Captive Portal,    * Metoda autoryzacji. 8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks. 9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC. 10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI. 11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. 12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. 13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV. 14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. 15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal. 16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. 17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. 18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. 19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. 20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP. |  |
|  | **Obsługa serwerów certyfikatów CA** | 1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. 2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:    * możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.    * możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.    * Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).    * usługę OCSP (Online Certificate Status Protocol). |  |
|  | **Obsługa serwerów DHCP** | 1. System musi posiadać funkcję zintegrowanego serwera DHCP. 2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. 3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:    * Uruchamianie usługi dla wybranych podsieci,    * Przypisanie ustalonego adresu IP dla adresu MAC.    * Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,    * Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,    * Możliwość określania braku dostępu dla wybranych adresów MAC,    * Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,    * Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,    * Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,    * Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,    * Dokonywanie zmian bez konieczności wyłączania usług. |  |
|  | **Obsługa serwerów TACACS+** | System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:   1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. 2. System musi umożliwiać tworzenia haseł administratorom. 3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów 4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. 5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. 6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory. 7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.   System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji |  |
|  | **Raportowanie i monitoring** | System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:   1. Monitoring autoryzacji. 2. Monitoring dla zdarzeń systemowych. 3. Monitoring dla zdarzeń DHCP. 4. Monitoring dla tożsamości. 5. Monitoring dla urządzeń końcowych. 6. Monitoring dla urządzeń sieciowych. 7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. 8. Raport ze zdarzeń logowania z informacją o nadam adresie IP. 9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. 10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. 11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. 12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. 13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. 14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. 15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. 16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi. 17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. 18. Raport zdarzeń Microsoft Active Directory, minimum:     * Logowania, wylogowania z system w tym błędne logowania     * Logowania do sieci 802.1X |  |
|  | **Alarmy** | 1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:    * wiadomości e-mail,    * Syslog,    * notyfikacji systemowych. 2. Alarmy mogą być generowane w sytuacjach, min:    * Ilości obsługiwanych transakcji RADIUS,    * Opóźnienie obsługi transkacji RADIUS,    * Statusu krytycznego modułów. 3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:    * badanie łączności IP za pomocą ping, traceroute,    * tcpdump protokołów RADIUS, TACACS+,    * wyszukiwanie zdarzeń RADIUS z uwzględnieniem:      + nazwy użytkownika,      + adresu MAC,      + statusu uwierzytelnienia (udana lub nieudana),      + powodu, jeżeli uwierzytelnienie nieudane,      + zakresu czasowego, co do dnia, godziny i minuty,    * wykonanie zdalnego polecenia na urządzeniu sieciowym. |  |
|  | **Wymagania dotyczące wdrożenia i harmonogram ramowy** | * Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta. * Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA). * Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.). * Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list). * Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach. * Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy. * Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy. * Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie. * Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia. |  |
|  | **Szkolenia/warsztaty:** | * Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC * Warsztaty zostaną przeprowadzone dla 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC * Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC * Warsztaty odbędą się w formie zdalnej. * Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej. * Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym |  |
|  | **Licencja wsparcia technicznego producenta oprogramowania:** | Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 24 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:   * Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC * Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia. * Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. * Dostęp do dokumentacji i instrukcji na stronie internetowej. * Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania. * Wykonawca będzie świadczył nieodpłatne usługi związane z aktualizacją i/lub zmianą platformy systemowej dla systemu NAC w okresie obowiązywania Umowy. |  |
|  | **Inne** | Jeśli zaproponowane przez Wykonawcę rozwiązanie wymaga dostarczenia środowiska serwerowego to musi ono spełniać minimalne parametry opisane w **Tabeli 4 pozycja 27 Inne wymagania** lub wyższe jeśli zaproponowany system będzie tego wymagał (*należy przewidzieć odpowiednia zwiększenie wydajności serwera z Tabeli 4 pozycja27* ). |  |

# Tabela 4 - System SIEM - 1 SZTUKA

|  |  |
| --- | --- |
| **PRODUCENT** |  |
| **MODEL** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **SYSTEM SIEM** | | | |
| **LP** | **Parametr** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | **Wymagania Ogólne** | 1. Dostawa 24-miesięcznej licencji oprogramowania dla systemu SIEM wraz z modułem SOAR. 2. Wdrożenie i konfiguracja systemu SIEM. 3. Dostawa, wdrożenie i konfiguracja darmowego skanera podatności open source. 4. Wdrożenie i konfiguracja modułu SOAR. 5. Przygotowanie i dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej, dokumentacji dla użytkownika, dokumentacji powdrożeniowej. 6. Szkolenie/warsztaty z obsługi SIEM i SOAR. 7. Zapewnienia 24-miesięcznej gwarancji dla systemu SIEM, SOAR i skanera podatności. 8. Zapewnienie usługi wsparcia technicznego dla systemu SIEM, SOAR i skanera podatności, w maksymalnej liczbie 300 godzin roboczych. |  |
|  | **Opis infrastruktury Zamawiającego** | | **Rodzaj urządzenia** | **Liczba** | | --- | --- | | Windows Active Directory Servers | 3 | | Windows IIS Servers | 4 | | Windows General Purpose Servers | 25 | | UNIX and Linux Servers | 24 | | DNS and DHCP Servers | 4 | | Antivirus Servers | 1 | | Database Servers | 11 | | Proxy Servers | 0 | | Firewalls | 1 | | IDS, IPS, and DAM | 1 | | VPNs | 2 | | Routers and Switches | 27 | | Microsoft 365 (Exchange, Teams, OneDrive itp.) | 20 użytkowników | | Total Workstations on Network | 250 | | Total Servers on Network | 70 | |  |
|  | **Słownik pojęć i skrótów** | | **Termin** | **Definicja** | | --- | --- | | Administrator systemu | Rola w systemie SIEM odpowiedzialna za konfigurację i bieżący nadzór nad prawidłowym działaniem systemu, posiadająca uprawnienia do akceptacji kluczowych operacji w systemie. | | Błąd Krytyczny/Awaria | Oznacza brak działania środowiska produkcyjnego systemu SIEM, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Błąd Krytyczny ma jedną lub więcej z poniższych cech:   1. Dane biznesowe zostały uszkodzone. 2. Funkcjonalność krytyczna systemu SIEM nie działa. 3. System w zakresie Funkcjonalności krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę lub procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu Gwarancji. 4. Wszelkie błędy związane z bezpieczeństwem przechowywania   i przetwarzania danych, które mogą wpłynąć na:   1. uwierzytelnianie, 2. niezaprzeczalność, 3. poufność, 4. integralność, 5. dostępność, 6. rozliczalność. 7. Wszelkie awarie związane z bezpieczeństwem dostępu do systemu SIEM (w tym nieautoryzowanym dostępem do danych).   Błąd Krytyczny/Awaria wymaga reakcji i naprawy z zachowaniem zdefiniowanego SLA. | | Błąd Drobny/  Usterka | Błąd uniemożliwiający wykonanie pewnego zadania, błędne działanie systemu SIEM, błąd, dla którego możliwe jest zastosowanie przebiegu alternatywnego:   1. Błędne działanie systemu SIEM. 2. Dotyczy funkcjonalności, która jest rzadziej używana. 3. Problemy niemające wpływu na ciągłość procesów biznesowych, powodujące uciążliwości w pracy systemu. 4. Błędy wydajnościowe, które zwalniają działanie systemu, ale nie blokują jego działania.   Błąd Drobny/Usterka wymaga reakcji i naprawy z zachowaniem zdefiniowanego SLA. | | Czas Naprawy | Czas liczony od momentu potwierdzenia przez Wykonawcę przyjęcia Zgłoszenia do momentu dostarczenia poprawki naprawiającej Błąd Krytyczny/Awarię lub Błąd Drobny/Usterkę lub wdrożenia Obejścia dla Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki. W przypadku dostarczenia poprawki lub wdrożenia Obejścia, które nie usuwają Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki Czas Naprawy uważa się za niedochowany. | | Czas Obejścia | Czas liczony od momentu skutecznego wdrożenia przez Wykonawcę Obejścia do momentu dostarczenia poprawki naprawiającej Błąd Krytyczny/Awarię lub Błąd Drobny/Usterkę. | | Czas Reakcji | Czas liczony od momentu przekazania przez Zamawiającego Zgłoszenia o Błędzie Krytycznym/Awarii lub Błędzie Drobnym/Usterce do momentu potwierdzenia przez Wykonawcę przyjęcia Zgłoszenia. | | Dzień Roboczy | Dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy w Polsce, w godz. 8:00 – 18:00. | | Dokumentacja | Wszelka dokumentacja dotycząca wdrażanego rozwiązania lub jakichkolwiek innych prac Wykonawcy, która jest dostarczana lub powstanie w ramach realizacji przedmiotu zamówienia, w tym np. dokumentacja analityczna, testowa, powykonawcza i eksploatacyjna. | | Funkcjonalność krytyczna | Funkcjonalność systemu SIEM istotna z punktu widzenia bezpieczeństwa oraz zachowania ciągłości działania systemu. | | Korelacja / korelacja zdarzeń | Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności. | | Niestandardowe źródło danych | Jest to źródło danych, dla którego system SIEM nie posiada gotowego mechanizmu integracji (parsera) lub wymaga on dostosowania do specyfiki źródła danych. | | Oprogramowanie standardowe | Oprogramowanie towarzyszące i niezbędne do funkcjonowania systemu będącego przedmiotem zamówienia, takie jak systemy operacyjne, wirtualizatory, systemy baz danych, systemy kopii zapasowych, systemy monitorowania, sterowniki itp. | | Oprogramowanie dedykowane | Oprogramowanie będące przedmiotem zamówienia: System SIEM wraz z modułem SOAR oraz skanerem podatności. | | System SIEM | (Security Information Event Management) system klasy SIEM, do którego głównych zadań należy gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. | | Wdrożenie | Doprowadzenie do uzyskania pełnej wymaganej przez Zamawiającego funkcjonalności systemu SIEM, SOAR, skanera podatności | | Wykonawca | Podmiot realizujący przedmiot zamówienia, wyłoniony w wyniku niniejszego postepowania zamówień publicznych. | | Zasób / Zasób IT | Elementy infrastruktury IT, z których system SIEM pozyskuje dane o zdarzeniach systemowych np. serwery (fizyczne i wirtualne), stacje robocze, urządzenia sieciowe, systemy teleinformatyczne, bazy danych, pliki itp. | | Zlecenie | Zlecenie składane przez Zamawiającego na realizację określonych prac dodatkowych w ramach usługi wsparcia. | | Zgłoszenie | Informacja przekazana Wykonawcy przez administratora systemu o Błędzie Krytycznym/Awarii, Błędzie Drobnym/Usterce lub Zleceniu. | | Źródła zdarzeń | Elementy infrastruktury IT, z których system SIEM wraz z modułem SOAR pozyskuje dane o zdarzeniach systemowych np. serwery (fizyczne i wirtualne), stacje robocze, urządzenia sieciowe, systemy teleinformatyczne, bazy danych, pliki itp. | |  |
|  | **Wymagania dla rozwiązania SIEM + SOAR** | 1. Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), którego celem jest gromadzenie i korelacja zdarzeń systemowych (w tym zdarzeń bezpieczeństwa), przesyłanych lub pobieranych z innych systemów i urządzeń teleinformatycznych. 2. System SIEM musi być kompatybilny z modułem obsługi incydentów SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń. 3. System SIEM i SOAR muszą być rozwiązaniem klasy enterprise, jednego producenta wraz z jego wsparciem. Nie dopuszcza się rozwiązań darmowych/open source oraz rozwiązań składających się z wielu osobnych modułów różnych producentów. 4. System SIEM musi pracować zachowując pełną funkcjonalność w modelu on premises w wyizolowanej infrastrukturze Zamawiającego. Zamawiający nie dopuszcza rozwiązań w modelu chmurowym. 5. System SIEM i SOAR musi umożliwiać instalację w wirtualnym środowisku VMware vSphere lub Microsoft HV. 6. Jeśli system nie zostanie dostarczony jako rozwiązanie sprzętowe, musi zostać dostarczony wraz z nim serwer o parametrach opisanych w pkt 27 wraz z niezbędnymi systemami i oprogramowaniem i licencjami. 7. Wszystkie komponenty wchodzące w skład Systemu SIEM i modułu SOAR muszą być w wersji produkcyjnej, implementowane w całości na maszynach wirtualnych w infrastrukturze Zamawiającego lub w postaci rozwiązań sprzętowych również umieszczonych w infrastrukturze Zamawiającego . Nie dopuszcza się rozwiązań chmurowych bądź częściowo chmurowych oraz komponentów w wersjach beta. 8. Wykonawca dostarczy najnowsze zalecane przez producenta wersje oprogramowania dla elementów Systemu SIEM oraz modułu SOAR na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez producenta rozwiązania. 9. System SIEM i SOAR muszą umożliwić, autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność, a także zapewniać poufność transmisji danych. 10. System SIEM i SOAR muszą posiadać graficzny interfejs użytkownika, możliwy do uruchomienia przez nowoczesną przeglądarkę internetową (Chrome, Edge, Firefox, Safari, Opera), bez konieczności instalowania dodatków do przeglądarki oraz innego dodatkowego oprogramowania. Nie dopuszcza się rozwiązań wymuszających wykorzystywanie niewspieranych przeglądarek i dodatków. 11. System SIEM musi gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem. 12. System SIEM i SOAR muszą umożliwiać równoczesną pracę 5 operatorów oraz objąć monitoringiem 500 zasobów IT. 13. System SIEM musi umożliwiać przetwarzanie zdarzeń w ilości 3 000 zdarzeń na sekundę. 14. Wszelkie dostarczone oprogramowania muszą posiadać licencje wieczyste. Zamawiający nie dopuszcza subskrypcji. 15. System SIEM musi przechowywać zgromadzone dane w wysokiej dostępności przez okres min. 90 dni oraz zapewniać automatyczną archiwizację po upływie tego terminu. 16. Wykonawca dostarczy, uruchomi i zintegruje z systemem SIEM darmowy skaner podatności open source. |  |
|  | **Wymagania funkcjonalne systemu SIEM + SOAR** | 1. System SIEM musi zapewniać odbiór lub pobieranie danych za pośrednictwem protokołów SYSLOG oraz NetFlow, mechanizmu Windows Event Forwarding (WEF) oraz sterownika ODBC lub JDBC. 2. System SIEM musi umożliwiać automatyczne pobieranie logów audytowych systemów baz danych. 3. System SIEM musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. 4. Proces normalizacji (parsowania) systemu SIEM musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 5. Normalizacja systemu SIEM musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól. 6. System SIEM musi posiadać predefiniowany zestaw reguł normalizacji (parsowania) logów dla popularnych źródeł logów takich jak: urządzenia sieciowe, systemy bezpieczeństwa, systemy Windows i Linux, Active Directory 7. System SIEM musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych system musi tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji. 8. System SIEM musi umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT poprzez wielowartościowe listy referencyjne i wykorzystywać je w regułach korelacyjnych. 9. System SIEM musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych, JSON lub XML. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia. 10. System SIEM musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej. 11. System SIEM musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych. 12. System SIEM musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej. 13. System SIEM musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. 14. Interfejs wyszukiwania systemu SIEM musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. 15. System SIEM powinien zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji. 16. System SIEM powinien być wyposażony w mechanizmy zautomatyzowanego, dynamicznego uzupełniania elektronicznej dokumentacji na podstawie danych pozyskanych z logów i informacji o ruchu sieciowym (Netflow), protokołów SNMP, WMI, SSH, skanerów podatności oraz skryptów PowerShell za pomocą których musi istnieć możliwość precyzyjnego określenia zakresu danych, które mają zostać uzupełnione. System musi posiadać repozytorium gotowych skryptów oraz graficzny interfejs pozwalający na tworzenie nowych skryptów, obejmujący możliwość przekazywania do nich parametrów wejściowych. 17. Mechanizmy automatycznego uzupełniania dokumentacji elektronicznej powinny uwzględniać informacje o typach zasobów (np. serwer WWW, baza danych, serwer plików, stacja robocza) oraz zależnościach między tymi zasobami (np.: stacja robocza łączy się do serwera baz danych). 18. Elektroniczna dokumentacja infrastruktury teleinformatycznej systemu SIEM powinna pozwalać na wprowadzenie informacji o procesach biznesowych oraz technicznych oraz określania powiązań procesów z elementami infrastruktury (np.: serwer X związany jest z procesami A i B). 19. Informacje o procesach biznesowych powinny uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00). 20. Interfejs systemu elektronicznej dokumentacji systemu SIEM powinien umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. 21. Wizualizacja powinna obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami. 22. Interfejs interaktywnej mapy sieci powinien umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji. 23. System powinien pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci. 24. System SIEM powinien umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej. 25. Interfejs systemu SIEM powinien pozwalać na manualne zmiany wartości parametrów obiektów, dodawanie obiektów oraz ich usuwanie, bezpośrednio z poziomu widoku mapy oraz tabeli. 26. System SIEM powinien prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je procesy techniczne i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians). 27. System SIEM musi umożliwiać wykrywanie topologii sieci fizycznej oraz jej wizualizacji na podstawie następujących protokołów sieciowych: SNMP v2 i v3, LLDP, CDP. 28. System elektronicznej dokumentacji systemu SIEM powinien zawierać bazę wiedzy eksperckiej uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą. 29. Interfejs elektronicznej dokumentacji systemu SIEM powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie ważnych procesów organizacji. 30. System SIEM dla zarejestrowanych zdarzeń/ incydentów, powinien automatycznie wyznaczać ścieżkę ataku i zaprezentować ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu. 31. System SIEM powinien pozwalać na automatyczne szacowanie ryzyka cyber zagrożeń dla wszystkich zasobów IT zdefiniowanych w elektronicznej dokumentacji infrastruktury teleinformatycznej. Szacowanie ryzyka musi uwzględniać architekturę sieci, typy zasobów informatycznych, zabezpieczenia oraz procesy i związane z nimi konsekwencje. 32. System SIEM powinien zapewniać narzędzia umożliwiające dokonanie oceny wpływu incydentu bezpieczeństwa IT na działalność organizacji (np.: system wyszukuje i prezentuje informacje nt. procesów organizacji i klasyfikowanych informacji, które mogły zostać naruszone w wyniku incydentu oraz wyświetla przewidywane istotne dla organizacji konsekwencje naruszenia bezpieczeństwa). 33. System SIEM powinien zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa oraz narzędzia umożliwiające definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewniać wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego. 34. System SIEM powinien posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. 35. Interfejs mapy sieci systemu SIEM powinien pozwalać m.in. na: 36. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny 37. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia 38. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia 39. wyświetlanie lokalizacji zasobów określonego rodzaju 40. wyświetlanie najbardziej narażonych zasobów teleinformatycznych 41. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie. 42. System SIEM powinien zapewniać graficzne narzędzia do definiowania wymagań bezpieczeństwa organizacji (m.in. środków ochrony wymaganych dla określonych elementów i obszarów systemu teleinformatycznego) oraz narzędzia do audytowania bezpieczeństwa względem tych wymagań. 43. Narzędzia systemu SIEM powinny umożliwiać m.in.: 44. wyznaczanie zasobów IT o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń, 45. wskazywanie zasobów IT o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń. 46. System SIEM powinien umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych). 47. System SIEM powinien umożliwiać uwzględnianie wyników szacowania ryzyka w mechanizmach korelacji zdarzeń. 48. System SIEM w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji musi umożliwiać automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email. 49. System SIEM musi pozwalać na prezentację danych w postaci tzw. „Dashboard”, tj. dostosowywać zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika. 50. System SIEM musi być wyposażony w moduł obsługi incydentów SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń. Moduł obsługi incydentów powinien stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania tego samego producenta. 51. Moduł obsługi incydentów systemu SIEM musi wspierać proces obsługi incydentów. W ramach procesu każdy incydent musi przejść proces selekcji, analizy, oceny wpływu i reakcji. W ramach procesu każdy incydent musi przyjmować stany właściwe dla etapów procesu obsługi incydentów np.: nowe zdarzenie, incydent, fałszywy alarm, incydent zamknięty. 52. Moduł obsługi incydentów musi umożliwiać przydzielanie zadań w ramach obsługi incydentu. 53. Moduł obsługi incydentów systemu SIEM musi zapewniać graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą m.in.: 54. wzbogacanie danych kontekstowych, 55. gromadzenie artefaktów danych związanych z incydentem 56. współpraca z innymi członkami zespołu, 57. komunikacja w ramach zespołu, 58. wykonywanie czynności związanych z reakcją na incydent 59. raportowanie przebiegu incydentu 60. Interfejs modułu obsługi incydentów systemu SIEM powinien prezentować dane na temat incydentu: 61. zdarzenia związane z incydentem, 62. informacje o zasobach związanych z incydentem na podstawie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej, 63. informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem, 64. informacje o zadaniach wyznaczonych w ramach obsługi incydentu, 65. listę powiązanych incydentów, 66. listę podatności zasobów związanych z incydentem. 67. Moduł obsługi incydentów systemu SIEM musi być wyposażony w mechanizm scenariuszy obsługi incydentów. 68. Moduł obsługi incydentów systemu SIEM musi posiadać mechanizmy automatycznego wykonania scenariuszy, elementów scenariuszy lub akcji. 69. Moduł obsługi incydentów systemu SIEM musi umożliwiać zmianę statusu incydentów na podstawie rezultatów akcji i elementów decyzyjnych scenariuszy. 70. Moduł obsługi incydentów systemu SIEM powinien być wyposażony w mechanizmy automatycznego dopasowania scenariuszy do incydentów. Dopasowanie musi uwzględniać co najmniej: 71. priorytet incydentu wynikający z rezultatów działania reguł korelacji zdarzeń, 72. ważność zasobu związanego z incydentem ustalana automatycznie na podstawie informacji uzyskanych z modułu dokumentacji elektronicznej, 73. typ zasobu, którego dotyczy incydent ustalony automatycznie na podstawie informacji pozyskanych z modułu dokumentacji elektronicznej, 74. aktualny status zdarzenia bądź incydentu w procesie obsługi incydentu. 75. Moduł obsługi incydentów systemu SIEM musi rejestrować wszystkie czynności wykonane przez użytkownika w ramach realizacji scenariuszy. 76. Moduł obsługi incydentów systemu SIEM musi być wyposażony w graficzny interfejs umożliwiający tworzenie i testowanie scenariuszy obsługi incydentów. 77. System SIEM powinien umożliwiać dokonanie zautomatyzowanej oceny wpływu incydentu bezpieczeństwa IT zidentyfikowanego przez mechanizmy korelacji SIEM na procesy określone w module elektronicznej dokumentacji infrastruktury teleinformatycznej. 78. Moduł obsługi incydentów systemu SIEM musi umożliwiać ustalanie przewidzianych czasów reakcji i czasów obsługi dla incydentów ze względu na ich priorytet. System musi dokonywać automatycznego pomiaru czasów reakcji na incydenty oraz czasów obsługi incydentów. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu. 79. Moduł obsługi incydentów systemu SIEM musi być wyposażony w mechanizm automatycznego powiadamiania wskazanych adresatów o nowych incydentach, zmianach statusów incydentów, przekroczeniach czasów reakcji i obsługi. 80. System SIEM lub SOAR musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: 81. ilość incydentów w czasie, w podziale na priorytety, 82. czasy reakcji i obsługi, 83. ilości incydentów obsługiwanych przez poszczególnych użytkowników. 84. System SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE. 85. System SIEM musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników. 86. Mechanizmy modułu dokumentacji elektronicznej systemu SIEM powinny umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności. 87. Moduł obsługi incydentów bezpieczeństwa systemu SIEM musi umożliwiać obsługę wykrytych podatności na zasadach zbliżonych do obsługi incydentów. Zasady te dotyczą w szczególności: 88. scenariuszy obsługi wraz z elementami decyzyjnymi i akcjami, 89. określenie statusu w ramach procesu obsługi (np.: nowa podatność, potwierdzona podatność, wymagana aktualizacja, akceptacja podatności itp.), 90. automatyczne ustalanie priorytetów podatności, 91. automatyczne mierzenie czasów reakcji i obsługi, 92. automatyczne powiadamianie (np.; przy pomocy email lub SMS), 93. automatyczne przydzielanie zespołu obsługi do podatności, 94. tworzenie i śledzenie zadań. 95. System SIEM musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamianie procesów skanowania i analizowania uzyskanych raportów. 96. System SIEM lub SOAR w formie graficznej musi prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności. 97. System SIEM musi zapewniać możliwość rozbudowy w przyszłości o dodatkowe moduły funkcjonalne. 98. Wykonawca dostarczy mechanizm (w postaci skryptu, bądź innego rozwiązania programowego) do archiwizacji całości systemu umożliwiającego odtworzenie kompletnego systemu. |  |
|  | **Wymagania dotyczące wdrożenia Etap 1** | 1. Wykonawca zapewni współpracę z Zamawiającym w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej systemu SIEM. 2. Wdrożenie systemu SIEM musi zostać wykonane we wskazanej przez Zamawiającego lokalizacji. 3. Wykonawca przedstawi projekt wdrożenia systemu SIEM w infrastrukturze Zamawiającego. 4. Wykonawca dostarczy licencję na oprogramowanie systemu SIEM i SOAR. 5. Wykonawca uruchomi system SIEM w całości na infrastrukturze Zamawiającego, w tymi: 6. przeprowadzi konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu SIEM, 7. zainstaluje i skonfiguruje niezbędne oprogramowanie standardowe oraz serwery wirtualne, 8. zainstaluje system SIEM, 9. zestawi połączenia zdalnego dostępu, 10. aktywuje licencje, 11. wykona konfigurację systemu SIEM. 12. Wykonawca podłączy wskazane przez Zamawiającego źródła zdarzeń. 13. Wykonawca dostarczy, uruchomi i zintegruje z systemem SIEM darmowy skaner podatności open source. 14. Wykonawca uruchomi i skonfiguruje parsery dla niestandardowych źródeł danych, jeżeli integracja ze wskazanymi przez Zamawiającego źródłami będzie tego wymagała. 15. Wykonawca uruchomi i skonfiguruje reguły korelacyjne, elektroniczną dokumentację infrastruktury, ustawienia i obszary bezpieczeństwa infrastruktury i sieci, mechanizmy oceny ryzyka, mechanizmy powiadamiania oraz obsługi incydentów. 16. Wykonawca dostroi i skalibruje reguły korelacji. 17. Wykonawca dostarczy dokumentację powdrożeniową oraz dokumentację systemu SIEM (techniczną oraz dla użytkownika). 18. Wykonawca zapewni transfer wiedzy w formie spotkania podsumowującego Etap 1 wdrożenia. |  |
|  | **Wymagania dotyczące wdrożenia Etap 2** | 1. Wykonawca uruchomi system SOAR w całości na infrastrukturze Zamawiającego, w tymi: 2. przeprowadzi konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu SOAR, 3. zainstaluje i skonfiguruje niezbędne oprogramowanie standardowe 4. zainstaluje system SOAR, 5. zestawi połączenia zdalnego dostępu, 6. aktywuje licencje, 7. wykona konfigurację systemu SOAR w tym uruchomi i skonfiguruje mechanizmy wykonywania scenariuszy automatyzacji SOAR. 8. Wykonawca dostarczy dokumentację powdrożeniową oraz dokumentację systemu SOAR (techniczną oraz dla użytkownika). 9. Wykonawca dokona niezbędnych integracji SOAR z innymi systemami w celu automatycznego wykonywania poleceń w ramach scenariuszy SOAR. 10. Wykonawca przeprowadzi szkolenia/warsztaty dla administratorów. 11. Wykonawca zapewni transfer wiedzy w formie spotkania podsumowującego Etap 2 wdrożenia. |  |
|  | **Wymagania w zakresie wsparcia technicznego** | 1. W ramach usługi wsparcia technicznego Wykonawca będzie zobowiązany do realizacji dodatkowych Zleceń, które będą wynikały z eksploatacji wdrożonych elementów przedmiotu zamówienia. 2. Całkowita liczba godzin Zleceń nie przekroczy 300 godzin roboczych. 3. Zgłoszenia będą dokonywane przez Zamawiającego w trybie NBD. 4. Zgłoszenia będą obsługiwane przez Wykonawcę w ramach zdefiniowanych parametrów SLA. 5. Zgłoszenia przekazywane przez Zamawiającego będą posiadały następujące kategorie: Błąd Krytyczny/Awaria, Błąd Drobny/Usterka, Zlecenie prac dodatkowych. 6. W ramach usługi wsparcia technicznego Wykonawca musi przeprowadzić analizę i implementację poprawek mających na celu przywrócenie funkcjonalności Systemu SIEM, SOAR lub skanera podatności w przypadku zaistnienia Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki. 7. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Systemu SIEM, SOAR lub skanera podatności, którego dotyczy Zgłoszenie, nie jest spowodowane Błędem Krytycznym/Awarią lub Błędem Drobnym/Usterką, za którą odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest: 8. wskazać przyczynę nieprawidłowego działania systemu poprzez wskazanie elementu, który ją powoduje, 9. udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji o systemie, potrzebnych do przywrócenia jego pełnej funkcjonalności. 10. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie systemu SIEM, SOAR lub skanera podatności spowodowane jest okolicznościami leżącymi po stronie Oprogramowania standardowego, wówczas Wykonawca nie jest zobowiązany do naprawy Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki, jeżeli nie jest w stanie jej wykonać ze względu na prawa osób trzecich. Wykonawca jest zobowiązany do dostarczenia Obejścia w Czasie Obejścia tak, aby zapewnić działanie systemu SIEM, SOAR lub skanera podatności mimo istnienia Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki w Oprogramowaniu standardowym. 11. Naprawa lub Obejście, które Wykonawca wdrożył, a które zostało odrzucona przez Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Błąd Krytyczny/Awaria lub Błąd Drobny/Usterka nadal występuje, trwa do czasu jego skutecznego wykonania. 12. Przez okres trwania Umowy Wykonawca zobowiązany jest przyjmować zapytania Zamawiającego dotyczące realizacji usług w ramach usług wsparcia technicznego. Zapytania składane będą: 13. za pośrednictwem aplikacji serwisowej (interfejsu helpdesk), 14. za pośrednictwem poczty elektronicznej na wskazany przez Wykonawcę adres email. 15. Zapytanie składane przez Zamawiającego będzie zawierać co najmniej: 16. Opis prac jakie Zamawiający chce zlecić. 17. Określenie oczekiwań Zamawiającego co do produktów i prac oraz sposobu ich wykonania i prowadzenia. 18. Termin zakończenia prac. 19. Inne kwestie istotne dla Zamawiającego. 20. Wykonawca udzieli odpowiedzi na zapytanie Zamawiającego w terminie 3 Dni Roboczych od dnia jego złożenia. 21. Odpowiedź na zapytanie zawierać będzie: 22. Propozycję sposobu wykonania zlecenia. 23. Termin wykonania prac. 24. Koszt wykonania prac. 25. Zamawiający w terminie 3 Dni Roboczych od dnia otrzymania odpowiedzi na zapytanie udzieli Zlecenia na wykonanie dodatkowych prac. 26. Brak ustosunkowania się przez Zamawiającego do odpowiedzi na zapytanie oznacza rezygnację z realizacji Zlecenia. 27. Realizacja Zlecenia potwierdzona będzie przez obie strony Protokołem Odbioru Miesięcznego za wsparcie. 28. Podstawą do ustalenia wysokości wynagrodzenia z tytułu Zlecenia będzie czasochłonność wykonania danego Zlecenia, zaakceptowana przez Zamawiającego. 29. Zamawiający dokona płatności jedynie za faktycznie wykorzystaną liczbę godzin prac zleconych. 30. Wykonawca musi zrealizować wszystkie złożone przez Zamawiającego Zlecenia. 31. Produkty wykonane lub dostarczone w ramach Zgłoszenia lub Zlecenia objęte zostaną Gwarancją, bez zmiany wysokości wynagrodzenia przysługującego Wykonawcy z tego tytułu. 32. Po przeprowadzeniu implementacji poprawek w ramach Zgłoszeń i realizacji Zleceń Wykonawca powinien uaktualnić Dokumentację w zakresie wykonanych zmian. |  |
|  | **Harmonogram ramowy**  **Etap I** | 1. Dostarczenie licencji na oprogramowanie systemu SIEM i SOAR. 2. Wdrożenie i konfiguracja systemu SIEM zgodnie z przedstawionymi wymaganiami. 3. Wdrożenie i konfiguracja skanera podatności zgodnie z przedstawionymi wymaganiami. 4. Dostarczenie dokumentacji przedwdrożeniowej oraz dokumentacji technicznej i dokumentacji użytkownika. |  |
|  | **Harmonogram ramowy**  **Etap II** | 1. Wdrożenie i konfiguracja systemu SOAR zgodnie z przedstawionymi wymaganiami 2. Dostarczenie dokumentacji powdrożeniowej zgodnie z przedstawionymi wymaganiami. 3. Przeprowadzenie szkolenia/warsztatu zgodnie z przedstawionymi wymaganiami. |  |
|  | **Szkolenia/warsztaty** | 1. Wykonawca zapewni bezpłatne 4-dniowe warsztaty (4 dni x 8h) w zakresie użytkowania i administrowania wdrożonym systemem SIEM i SOAR. 2. Warsztaty zostaną przeprowadzone dla łącznie 5 osób i będą uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządzanie incydentami bezpieczeństwa, korzystanie ze scenariuszy obsługi incydentów, kompletowanie informacji potrzebnych do opracowania raportu o incydencie, szacowanie ryzyka, itp.). 3. Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu SIEM i SOAR. 4. Warsztaty odbędą się w siedzibie Zamawiającego lub, w formie zdalnej jeśli tak zdecyduje Zamawiający. 5. Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej. 6. Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym. |  |
|  | **Dokumentacja** | 1. Wykonawca dostarczy dokumentację obejmującą: 2. projekt wdrożenia rozwiązania w infrastrukturze Zamawiającego, 3. dokumentacja powdrożeniową, 4. dokumentację techniczną umożliwiająca Zamawiającemu samodzielną administracje rozwiązaniem 5. dokumentację użytkownika, zawierającą typowe scenariusze użycia SIEM i SOAR,   a także przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji.   1. Wszelka dokumentacja wytworzona przez Wykonawcę musi być sporządzona w języku polskim. 2. Dokumentacja musi być w formacie Microsoft Word z obsługą trybu rejestracji zmian. 3. Wszelka dokumentacja musi charakteryzować się wysoką jakością i czytelnością. 4. Dodatkowe formaty zapisu dokumentacji np. diagramy UML lub formaty wektorowe należy dołączyć na odrębnym nośniku danych. Pliki powinny być możliwe do otwarcia/importu przez: MS Project, MS Visio. |  |
|  | **Procedury odbioru** | 1. Dostawa licencji na oprogramowanie systemu SIEM wraz z modułem SOAR. 2. Wdrożenie i konfiguracja systemu SIEM. 3. Dostawa, wdrożenie i konfiguracja darmowego skanera podatności open source. 4. Wdrożenie i konfiguracja modułu SOAR. 5. Dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej, dokumentacji dla użytkownika, dokumentacji powdrożeniowej. 6. Szkolenie/warsztaty z obsługi SIEM i SOAR. |  |
|  | **Wymagania ogólne – Procedury Odbioru** | 1. Odbiór każdego elementu realizacji przedmiotu zamówienia dotyczący wdrożenia i konfiguracji oprogramowania musi być potwierdzony Protokołem Odbioru Jakościowego. 2. Odbiór poszczególnych elementów realizacji przedmiotu zamówienia musi następować po kolei zgodnie z harmonogramem ramowym. 3. Odbiór dokumentacji musi być potwierdzony Protokołem Odbioru Dokumentacji. 4. Odbiór licencji musi być potwierdzony Protokołem Odbioru Ilościowego. 5. Odbiór szkoleń w formie warsztatów musi być potwierdzony Protokołem Odbioru Szkolenia. 6. Odbiór Zleceń wykonania prac dodatkowych w ramach Usług wsparcia technicznego musi być potwierdzony Protokołem Odbioru Miesięcznego za wsparcie. 7. Odbiór końcowy przedmiotu zamówienia musi być potwierdzony Protokołem Odbioru Końcowego. |  |
|  | **Procedura odbioru Etap 1** | 1. W etapie 1 zostanie zrealizowane:   1. Dostarczenie licencji na oprogramowanie systemu SIEM i SOAR. 2. Wdrożenie i konfiguracja systemu SIEM. 3. Wdrożenie i konfiguracja skanera podatności. 4. Dostarczenie dokumentacji przedwdrożeniowej oraz dokumentacji technicznej i dokumentacji użytkownika dla systemu SIEM. 5. Odbiór dostarczonych dokumentów potwierdzony zostanie Protokołem Odbioru Dokumentacji. 6. Odbiór dostarczonych licencji potwierdzony zostanie Protokołem Ilościowym. 7. Odbiór wdrożenia systemu SIEM zostanie potwierdzony Protokołem Odbioru Jakościowego. 8. Odbiór wdrożenia skanera podatności zostanie potwierdzony Protokołem Odbioru Jakościowego. |  |
|  | **Procedura odbioru Etap 2** | 1. W etapie 2 zostanie zrealizowane: 2. Wdrożenie i konfiguracja systemu SOAR zgodnie z przedstawionymi wymaganiami 3. Dostarczenie dokumentacji powdrożeniowej zgodnie z przedstawionymi wymaganiami 4. Przeprowadzenie szkolenia/warsztatu zgodnie z przedstawionymi wymaganiami. 5. Odbiór dostarczonych dokumentów potwierdzony zostanie Protokołem Odbioru Dokumentacji. 6. Odbiór wdrożenia systemu SOAR zostanie potwierdzony Protokołem Odbioru Jakościowego. 7. Odbiór szkoleń w formie warsztatów zostanie potwierdzony Protokołem Odbioru Szkolenia. 8. Odbiór końcowy przedmiotu zamówienia musi być potwierdzony Protokołem Odbioru Końcowego. |  |
|  | **Procedury Odbioru – Odbiór jakościowy** | 1. Na 3 Dni Robocze przed terminem odbioru jakościowego, Wykonawca zobowiązany jest przekazać informację o planowanym odbiorze oraz osobach realizujących odbiór jakościowy. 2. Odbiór wdrożenia i konfiguracji systemu SIEM, SOAR oraz skanera podatności będzie polegał na sprawdzeniu przez Wykonawcę w obecności Zamawiającego poprawności działania zainstalowanego oprogramowania oraz zgodności działania i konfiguracji z wymaganiami Zamawiającego. 3. Odbiór wdrożenia i konfiguracji systemu SIEM, SOAR oraz skanera podatności potwierdzony zostanie Protokołem Jakościowym, w którym Zamawiający określa czy: a) Odbiera wdrożenie systemu SIEM bez zastrzeżeń. b) Odbiera wdrożenie systemu SIEM z zastrzeżeniami. 4. W przypadku uwag do odbioru jakościowego, Zamawiający dołącza do Protokołu Jakościowego ich wykaz. 5. Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Jakościowego z zastrzeżeniami. 6. Ostateczną datą odbioru jakościowego jest data podpisania Protokołu Odbioru Jakościowego bez zastrzeżeń. |  |
|  | **Procedury odbioru – odbiór dokumentacji** | 1. Wykonawca, z 3 dniowym wyprzedzeniem, zobowiązany jest przekazać informację o planowanym terminie przekazania Dokumentacji do akceptacji 2. Dla Dokumentacji zawierającej maksymalnie 300 stron, w terminie 5 Dni Roboczych od dnia przekazania Dokumentacji, Zamawiający przekazuje Wykonawcy Protokół Odbioru Dokumentacji, w którym określa czy: a) Odbiera Dokumentację bez zastrzeżeń. b) Odbiera Dokumentację z zastrzeżeniami. 3. Dla Dokumentacji zawierającej więcej niż 300 stron, termin odbioru Dokumentacji zostanie ustalony wspólnie przez Zamawiającego i Wykonawcę, jednak nie może być on dłuższy niż 10 Dni Roboczych. 4. W przypadku uwag do Dokumentacji, Zamawiający dołącza do Protokołu Odbioru Dokumentacji ich wykaz. 5. Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag i przekazać poprawioną Dokumentację wraz z odniesieniem się do uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Dokumentacji z zastrzeżeniami. 6. Ostateczną datą odbioru Dokumentacji jest data podpisania Protokołu Odbioru Dokumentacji bez zastrzeżeń. |  |
|  | **Procedury odbioru – odbiór szkolenia / warsztatu** | 1. Do Protokołu Odbioru Szkolenia Wykonawca musi dołączyć listy obecności uczestników szkolenia/warsztatów oraz kopie imiennych zaświadczeń o ukończeniu szkolenia/warsztatów wszystkich uczestników. 2. Zakończenie Szkolenia w formie warsztatów potwierdzone zostanie Protokołem Odbioru Szkolenia, w którym Zamawiający określa czy: 3. Odbiera szkolenia/warsztaty bez zastrzeżeń. 4. Odbiera szkolenia/warsztaty z zastrzeżeniami. 5. Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Szkolenia z zastrzeżeniami. 6. Ostateczną datą odbioru szkoleń/warsztatów jest data podpisania Protokołu Odbioru Szkolenia bez zastrzeżeń. |  |
|  | **Procedury odbioru – odbiór końcowy** | 1. Kryterium odbioru końcowego systemu SIEM, SOR oraz skanera podatności będzie podpisanie bez zastrzeżeń: Protokołów Odbioru Jakościowego, Protokołów Odbioru Ilościowego, Protokołów Odbioru Dokumentacji, Protokołów Odbioru szkolenia z realizacji każdego Etapu przedmiotu zamówienia. 2. Odbiór końcowy potwierdzony zostanie Protokołem Odbioru Końcowego w którym Zamawiający określa czy: 3. Dokonuje odbioru przedmiotu zamówienia bez zastrzeżeń. 4. Dokonuje odbioru przedmiotu zamówienia z zastrzeżeniami. 5. W przypadku uwag do odbioru końcowego, Zamawiający dołącza do Protokołu Odbioru Końcowego ich wykaz. 6. Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Końcowego z zastrzeżeniami. 7. Ostateczną datą odbioru końcowego jest data podpisania Protokołu Odbioru Końcowego bez zastrzeżeń. |  |
|  | **Procedura Odbioru – Usługi wsparcia technicznego** | 1. Odbiór zrealizowanego przez Wykonawcę przedmiotu Zlecenia odbędzie się Protokołem Odbioru Zlecenia na podstawie przeprowadzonych procedur weryfikacji wykonania Zlecenia. 2. W przypadku konieczności przeprowadzenia dodatkowych odbiorów danego Zlecenia (np. w zakresie testów akceptacyjnych, odbiorów jakościowych, odbiorów częściowych) poprzedzających procedurę odbioru Zlecenia procedura dodatkowych odbiorów zostanie opisana w formularzu Zlecenia. 3. W pracach związanych z dokonywaniem czynności odbiorczych zobowiązany jest uczestniczyć przedstawiciel Wykonawcy. Zamawiający dopuszcza formę zdalną / online obecności przedstawiciela Wykonawcy. |  |
|  | **Gwarancja - Wymagania ogólne** | 1. Wykonawca udzieli 24-miesięcznej Gwarancji na dostarczone systemy SIEM i SOAR oraz skaner podatności. 2. Wykonawca zapewni 24-miesięczną Gwarancję producenta na Oprogramowanie Standardowe. 3. Wykonawca udzieli 24-miesięcznej rękojmi na: Oprogramowanie standardowe. Oprogramowanie dedykowane (SIEM, SOAR i skaner podatności). 4. Wykonawca będzie świadczył usługi wsparcia technicznego dla systemu SIEM i SOAR wraz ze skanerem podatności w okresie obowiązywania Umowy. 5. Wykonawca będzie świadczył nieodpłatne usługi związane z aktualizacją i/lub zmianą platformy systemowej dla systemu SIEM i SOAR wraz ze skanerem podatności w okresie obowiązywania Umowy. 6. Gwarancja na Oprogramowanie standardowe będzie liczona od dnia podpisania Protokołu Odbioru Jakościowego systemu SIEM. 7. Gwarancja na dostarczone Oprogramowanie SIEM, SOAR oraz skaner podatności będzie liczona od dnia podpisania Protokołu Odbioru Jakościowego systemu SIEM. 8. Rękojmia będzie liczona od dnia podpisania Protokołu Odbioru Jakościowego systemu SIEM. 9. Błędy Krytyczne i Błędy Drobne Oprogramowania dedykowanego i Oprogramowania standardowego będą usuwane zgodnie z warunkami producenta, przy czym warunki te nie mogą być gorsze niż wymagania dotyczące Gwarancji. 10. Zakres świadczeń w ramach Gwarancji obejmuje: 11. Usuwanie Błędów Krytycznych i Błędów Drobnych Oprogramowania standardowego oraz Oprogramowania SIEM, SOAR oraz skanera podatności zgodnie z Czasami Reakcji, Czasami Naprawy, Czasami Obejścia i Maksymalnymi czasami Obejścia dla poszczególnych kategorii błędów. 12. Dostarczanie, instalację i konfigurację nowych wersji Oprogramowania standardowego oraz Oprogramowania SIEM, SOAR oraz skanera podatności. 13. Prowadzenie wszelkich działań prewencyjnych mających na celu wydłużenie czasu bezawaryjnej pracy przedmiotu zamówienia. 14. Odzyskiwanie danych systemu SIEM i SOAR utraconych lub uszkodzonych w wyniku Błędów Krytycznych/Awarii i Błędów Drobnych/Usterek Oprogramowania Standardowego lub Oprogramowania SIEM, SOAR oraz skanera podatności. 15. Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych w systemie SIEM. 16. Wykonawca w ramach Gwarancji pokryje wszystkie koszty związane z naprawą, m.in. koszty transportu, ubezpieczenia, robocizny. |  |
|  | **Gwarancja – Oprogramowanie standardowe** | 1. Wykonawca zapewni elektroniczny dostęp do informacji na temat posiadanego Oprogramowania standardowego oraz biuletynów technicznych, poprawek, aktualizacji, nowych wersji Oprogramowania standardowego. 2. Wykonawca w przypadku Oprogramowania standardowego: 3. Opracowuje i uzgadnia z Zamawiającym plan obsługi serwisowej (raz w roku). 4. Dostarcza aktualizacje, nowe wersje oraz zmiany w Oprogramowaniu standardowym, opracowane przez producenta podczas trwania Gwarancji. 5. Zapewnia, że dostarczane aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim. 6. W ciągu każdego roku trwania Umowy opracowuje plan aktualizacji Oprogramowania standardowego. 7. Informuje o najlepszych praktykach i zasadach postępowania. 8. Wykonawca musi zapewnić wsparcie producenta w przypadku gdy zgodnie z licencją producenta dostęp do aktualizacji Oprogramowania standardowego takiego wsparcia wymaga. 9. Wykonawca musi zapewnić subskrypcje Oprogramowania standardowego w przypadku gdy są one niezbędne do poprawnego działania wymaganych funkcjonalności systemu. |  |
|  | **Gwarancja – Oprogramowanie SIEM, SOAR i skaner podatności** | 1. Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie Oprogramowania SIEM, SOAR oraz skaner podatności będącego przedmiotem zamówienia. 2. Po usunięciu każdego Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki Wykonawca zobowiązany jest do przywrócenia prawidłowego funkcjonowania Oprogramowania SIEM, SOAR oraz skanera podatności. |  |
|  | **SLA** | 1. SLA dla oprogramowania będzie liczone w okresie jednego roku. 2. W uzasadnionych przypadkach Zamawiający wraz z Wykonawcą mogą podjąć decyzję o wydłużeniu Czasu Naprawy, Czasu Obejścia, Maksymalnego czasu Obejścia. 3. Okna serwisowe związane z konserwacją/naprawą/rekonfiguracją Sytemu nie podlegają uwzględnianiu w obliczeniu SLA. Termin i zakres prac realizowanych w ramach okna serwisowego wymaga uzyskania przez Wykonawcę uprzedniej akceptacji Zamawiającego.  | Kategoria | Czas Reakcji | Czas Naprawy | Czas Obejścia | Maksymalny czas Obejścia | | --- | --- | --- | --- | --- | | Błąd Krytyczny/Awaria | 2 godziny w Dniu Roboczym | 48 godzin | 12 godzin | 7 Dni Roboczych | | Błąd Drobny/Usterka | 2 godziny w Dniu Roboczym | 72 godziny | 12 godzin | 14 Dni Roboczych | |  |
|  | Bezpieczeństwo przetwarzanych danych | 1. Wykonawca zobowiązany jest do przestrzegania, przekazanych w trakcie realizacji przedmiotu zamówienia, zasad i przepisów dotyczących bezpieczeństwa informacji oraz systemów informatycznych, obowiązujących u Zamawiającego, oraz innych zasad związanych z wykonywaniem czynności na terenie obiektów Zamawiającego. Zobowiązanie to dotyczy wszystkich osób, z pomocą których Wykonawca będzie realizował przedmiot zamówienia. 2. System SIEM musi być w pełni zgodny z zasadami bezpieczeństwa zdefiniowanymi w przekazanych przez Zamawiającego instrukcjach i procedurach. Z uwagi na zakres Polityki Bezpieczeństwa Danych Osobowych (PBDO) Zamawiającego, zasady i reguły określone w PBDO podlegają ochronie przed ujawnieniem lub udostępnieniem nieupoważnionej lub nieuprawnionej osobie lub nieuprawnionemu podmiotowi zewnętrznemu, dlatego dokumenty te zostaną przekazane Wykonawcy po podpisaniu Umowy na realizację przedmiotu zamówienia. 3. Przesyłanie danych w obrębie systemu SIEM i SOAR musi odbywać się w dedykowanej sieci Zamawiającego - bezpiecznymi kanałami, szyfrowanymi i chronionymi przed nieuprawnionym dostępem oraz zapewniającymi poufność, integralność i dostępność danych osobowych. 4. Wszystkie dane, które będą udostępnione w systemie SIEM i SOAR muszą być chronione przed nieuprawnionym odczytem poprzez mechanizmy logowania z wykorzystaniem unikalnego identyfikatora oraz hasła. Wytyczne dotyczące sposobu budowania identyfikatorów i haseł zostaną przekazane przez Zamawiającego. 5. System SIEM i SOAR musi zapewniać logowanie wszystkich udanych i nieudanych prób dostępu do systemu z uwzględnieniem informacji o użytkowniku końcowym, dacie i czasie logowania oraz adresu IP z którego nastąpiła próba logowania. 6. System SIEM i SOAR musi umożliwiać pełną identyfikację użytkownika końcowego i czasu wykonania każdej zmiany w bazie danych systemu, w szczególności operacji wstawiania rekordów, aktualizacji rekordów, tak aby zagwarantować pełną rozliczalność systemu. |  |
|  | **Zobowiązania Wykonawcy** | 1. Przedmiot zamówienia musi zostać zrealizowany przez Wykonawcę z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową. 2. Całość Przedmiotu zamówienia musi zostać zrealizowana zgodnie z terminami określonymi w OPZ. 3. Wykonawca jest zobowiązany do dokonywania wszelkich niezbędnych ustaleń mogących wpływać na Przedmiot Zamówienia z Zamawiającym. 4. Wykonawca sprawnie i terminowo zrealizuje Przedmiot zamówienia, w tym uwzględni w trakcie jego realizacji wszystkie uwagi zgłaszane przez Zamawiającego. 5. Wykonawca, na każdym etapie umowy, udzieli Zamawiającemu wszelkich informacji na temat stanu realizacji Przedmiotu zamówienia. |  |
|  | **Zobowiązania Zamawiającego** | 1. Udostępnienia wszelkich materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, które są niezbędne celem realizacji Przedmiotu zamówienia. 2. Informowania Wykonawcy o wszelkich czynnościach, które mogą mieć wpływ na realizację Przedmiotu zamówienia przez Wykonawcę. 3. Udostępnienia obiektów, sprzętu, oprogramowania i dokumentacji, które są niezbędne do realizacji Przedmiotu zamówienia zgodnie z polityką bezpieczeństwa i regulacjami wewnętrznymi, obowiązującymi u Zamawiającego. |  |
|  | **Inne wymagania** | **Jeśli zaproponowany system nie będzie dostarczony jako rozwiązanie sprzętowe należy dostarczyć serwer Rack o parametrach sprzętowych nie mniejszych niż (lub wyższych jeśli zaproponowany system będzie tego wymagał):**  • Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.  • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.  • Płyta główna z możliwością zainstalowania do dwóch procesorów.  • Obsługa procesorów 32 rdzeniowych.  • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.  • Płyta główna powinna obsługiwać do 1TB pamięci RAM.  • Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.  • Dwa procesory 16-rdzeniowe, min. 2.0GHz, umożliwiające osiągnięcie wyniku min. 265 w teście SPECrate2017\_int\_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej  • Minimum 256GB DDR5 RDIMM 5600MT/s,  • Demand Scrubing,  • Patrol Scrubing,  • Permanent Fault Detection  • minimum trzy sloty PCIe  • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)  • Dwie, dwuportowe karty sieciowe 25Gb Ethernet SFP28  • 16x wkładka 25GbE SFP28 SR dedykowana do oferowanych kart SFP28  • Zainstalowane:  • 4x dysk SSD SATA MU o pojemności min. 960GB, 12Gb, 2,5“ Hot-Plug.  • Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.  • Sprzętowy kontroler dyskowy, posiadający  • Min. 8GB nieulotnej pamięci cache,  • Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  • Wsparcie dla dysków samoszyfrujących.  • 4 x USB z czego nie mniej niż 1x USB 3.0,  • 2x VGA  • Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200  • Redundantne, Hot-Plug min. 1100W klasy Titanium  • Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  • Moduł TPM 2.0  • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem  • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).  • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:  • zdalny dostęp do graficznego interfejsu Web karty zarządzającej;  • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);  • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;  • możliwość podmontowania zdalnych wirtualnych napędów;  • wirtualną konsolę z dostępem do myszy, klawiatury;  • wsparcie dla IPv6;  • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;  • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;  • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;  • integracja z Active Directory;  • możliwość obsługi przez dwóch administratorów jednocześnie;  • wsparcie dla dynamic DNS;  • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.  • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera  • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera  •  • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej  • Przesyłanie danych telemetrycznych w czasie rzeczywistym  • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze  • Automatyczna rejestracja certyfikatów (ACE)  • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:  • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  • integracja z Active Directory  • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish  • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  • Szczegółowy opis wykrytych systemów oraz ich komponentów  • Możliwość eksportu raportu do CSV, HTML, XLS, PDF  • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.  • Grupowanie urządzeń w oparciu o kryteria użytkownika  • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji  • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  • Szybki podgląd stanu środowiska  • Podsumowanie stanu dla każdego urządzenia  • Szczegółowy status urządzenia/elementu/komponentu  • Generowanie alertów przy zmianie stanu urządzenia.  • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń  • Integracja z service desk producenta dostarczonej platformy sprzętowej  • Możliwość przejęcia zdalnego pulpitu  • Możliwość podmontowania wirtualnego napędu  • Kreator umożliwiający dostosowanie akcji dla wybranych alertów  • Możliwość importu plików MIB  • Przesyłanie alertów „as-is” do innych konsol firm trzecich  • Możliwość definiowania ról administratorów  • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów  • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta  • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów  • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.  • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.  • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile  • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.  • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.  • Zdalne uruchamianie diagnostyki serwera.  • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.  • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.  • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001  • Serwer musi posiadać deklaracja CE.  • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.  • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.  • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.  • Oferowany serwer musi być dostarczony wraz z licencjami umożliwiającymi uruchomienie 4 maszyn wirtualnych Microsoft Windows Server 2022  • Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  • Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 36 miesięcy.  • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)  • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.  • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.  • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.  • Zamawiający wymaga, aby Serwis urządzeń był realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |  |

# Tabela 5 - System analizy ruchu sieci - 1 SZTUKA

|  |  |
| --- | --- |
| **PRODUCENT** |  |
| **MODEL** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **SYSTEM ANALIZY RUCHU SIECI** | | | |
| **LP** | **Parametr** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | **Wymagania Ogólne** | W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych z zapór UTM będących przedmiotem postępowania.  Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7…, 8…; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016, 2019, 2022; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP). |  |
|  | **Interfejsy, Dysk** | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB. |  |
|  | **Parametry wydajnościowe** | 1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.   W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: |  |
|  | **Logowanie** | 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:   a. Listę najczęściej wykrywanych ataków.  b. Listę najbardziej aktywnych użytkowników.  c. Listę najczęściej wykorzystywanych aplikacji.  d. Listę najczęściej odwiedzanych stron www.  e. Listę krajów , do których nawiązywane są połączenia.  f. Listę najczęściej wykorzystywanych polityk Firewall.  g. Informacje o realizowanych połączeniach IPSec.   1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
|  | **Raportowanie** | W zakresie raportowania system musi zapewniać:  1. Generowanie raportów co najmniej w formatach: PDF, CSV.  2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.  3. Funkcję definiowania własnych raportów.  4. Możliwość spolszczenia raportów.  5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
|  | **Korelacja logów** | W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:  * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.  1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. |  |
|  | **Zarządzanie** | 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. 2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
|  | **Serwisy, licencje** | 1. Wykonawca musi zapewnić wdrożenie systemu oraz instruktarz z administracji wykonane przez inżyniera posiadającego aktualny certyfikat techniczny producenta oferowanego systemu. Dopuszczalna jest forma zdalna dla tego wdrożenia. 2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wymagane jest posiadanie co najmniej dwóch osób wyznaczonych do realizacji zamówienia z aktualnym certyfikatem producenta oferowanego rozwiązania. W tym celu wykonawca musi posiadać co najmniej dwóch inżynierów (wyznaczonych do realizacji prac związanych z wdrożeniem) posiadających aktualny certyfikat techniczny lub certyfikaty wystawione przez producenta oferowanego rozwiązania potwierdzające wiedzę i obsługę z ich zakresu. Na wezwanie Zamawiającego Wykonawca jest zobowiązany przedstawić przed rozpoczęciem prac wymagane dokumenty. |  |
|  | **Gwarancja** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w ciągu 7 dni roboczych. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |
|  | **Inne wymagania** | Jeśli zaproponowane przez Wykonawcę rozwiązanie wymaga dostarczenia środowiska serwerowego to musi ono spełniać minimalne parametry opisane w **Tabeli 4 pozycja 27 Inne wymagania** lub wyższe jeśli zaproponowany system będzie tego wymagał (*należy przewidzieć odpowiednia zwiększenie wydajności serwera z Tabeli 4 pozycja27* ). |  |

# Tabela 6 - Urządzenie UTM - 4 SZTUKI

|  |  |
| --- | --- |
| **PRODUCENT** |  |
| **MODEL** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **URZĄDZENIE UTM** | | | |
| **LP** | **Parametr** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry techniczne** |
|  | **Wymagania Ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |  |
|  | **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |  |
|  | **Interfejsy, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45, Dodatkowo wymagane są dwa porty 10Gb SFP+, przy czym mogą być one portami współdzielonymi zamiennie z wymaganymi portami 1Gb 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 20 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC. |  |
|  | **Parametry wydajnościowe** | 1. W zakresie Firewall’a obsługa nie mniej niż 1 milion. jednoczesnych połączeń oraz 100 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 25 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2,5 Gbps. |  |
|  | **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system |  |
|  | **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. |  |
|  | **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
|  | **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
|  | **Funkcje SD-WAN** | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. |  |
|  | **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
|  | **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
|  | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
|  | **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
|  | **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
|  | **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
|  | **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
|  | **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze oraz w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
|  | **Certyfikaty** | 1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall. |  |
|  | **Serwisy, licencje, wsparcie** | 1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, chmurowa platforma logowania z roczną retencją logów na okres 36 miesięcy. 2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wymagane jest posiadanie co najmniej dwóch osób wyznaczonych do realizacji zamówienia z aktualnym certyfikatem producenta oferowanego rozwiązania. W tym celu wykonawca musi posiadać co najmniej dwóch inżynierów (wyznaczonych do realizacji prac związanych z wdrożeniem) posiadających aktualny certyfikat techniczny lub certyfikaty wystawione przez producenta oferowanego rozwiązania potwierdzające wiedzę i obsługę z ich zakresu. Na wezwanie Zamawiającego Wykonawca jest zobowiązany przedstawić przed rozpoczęciem prac wymagane dokumenty. |  |
|  | **Gwarancja** | 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w ciągu 7 dni roboczych. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |
| **21.** | **Dodatkowe usługi zakres prac związanych z montażem, instalacją** | Zamawiający wymaga:   1. Przeprowadzenia przez Wykonawcę audytu istniejących urządzeń UTM u Zamawiającego pod kątem dobrych praktyk i poprawności pracy. 2. Opracowania przez Wykonawcę na podstawie wyników audytu i w konsultacji z Zamawiającym projektu technicznego wdrożenia, obejmującego między innymi:    1. Instalację dostarczonych urządzeń UTM.    2. Przeniesienie istniejących konfiguracji na nowe urządzenia z uwzględnieniem audytu, dobrych praktyk i poprawności pracy.    3. Konfigurację zarządzania (SSH, HTTPS, SNMP).    4. Konfigurację logowania zdarzeń.    5. Opracowanie scenariuszy testów akceptacyjnych. 3. Wdrożenia urządzeń UTM zgodnie z opracowanym projektem technicznym. 4. Realizacji testów akceptacyjnych. |  |

**Wymagania ogólne dla całości usług wdrożenia i konfiguracji środowiska serwerowego i sieciowego:**

1. Zamawiający wymaga opracowania projektu technicznego wdrożenia przed rozpoczęciem prac wdrożeniowych, w konsultacji z Zamawiającym.
2. Zamawiający wymaga, aby prace wdrożeniowe skutkujące niedostępnością infrastruktury IT Zamawiającego były realizowane po godzinach pracy, tj. w godzinach 16:00-8:00 w dni robocze oraz w weekendy (całą dobę)
3. Zamawiający wymaga, aby wdrożony sprzęt i oprogramowanie było zaktualizowane do najnowszej dostępnej i stabilnej wersji (dotyczy w szczególności oprogramowania układowego i sterowników), w konsultacji z Zamawiającym.
4. Zamawiający wymaga opracowania dokumentacji powykonawczej wdrożenia, obejmującej całość wykonanych prac, w tym dokumentację zmian w infrastrukturze zależnej.
5. Zamawiający wymaga dostarczenia wraz z zaoferowanym sprzętem kompletnego okablowania niezbędnego do poprawnego zainstalowania i skonfigurowania całości proponowanego rozwiązania.
6. Zamawiający dopuszcza instalacje zaproponowanych systemów na jednym serwerze spełniających minimalne parametry opisane w **Tabeli 4 pozycja 27 (Inne wymagania**) lub wyższe jeśli zaproponowany system będzie tego wymagał (należy przewidzieć odpowiednia zwiększenie wydajności serwera z Tabeli 4 pozycja27 ).

**Harmonogram dostaw**

|  |  |
| --- | --- |
| **ETAP** | **Czynności** |
| **I** | **Instalacja i wdrożenie sprzętu z Tabeli 1 i Tabeli 2** |
| **II** | **Instalacja i wdrożenie systemu NAC z Tabeli 3** |
| **III** | **Instalacja i wdrożenie systemu analizy ruchu sieci z Tabeli 5** |
| **IV** | **Instalacja i wdrożenie systemu SIEM z Tabeli 4** |
| **V** | **Instalacja i wdrożenie systemów UTM z Tabeli 6** |

Uwaga: Wszystkie podzespoły muszą być fabrycznie nowe, pochodzące z bieżącej produkcji, kompletne, sprawne technicznie, wyprodukowane nie wcześniej niż w 2023 r., nieuszkodzone mechanicznie oraz elektronicznie.