***Załącznik Nr 1 do SWZ***

**Zamówienie finansowane ze środków FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.**

**Opis przedmiotu zamówienia (OPZ)**

Nazwa zamówienia: Gmina Michałów

Zamawiający: Gmina Michałów, Michałów 115, 28-411 Michałów

Spis Treści:

**1. Switch - Przełącznik sieciowy zarządzalny.**

**2. System zabezpieczenia danych przed wyciekiem informacji.**

**3. Urządzenie z systemem do ochrony poczty elektronicznej.**

**4. System kontroli i zarządzania dostępem do sieci (System NAC).**

**5. System SIEM do analizy oraz zarządzania logami.**

**6. Wznowienie licencji fizycznego UTM.**

**1. Switch - Przełącznik sieciowy zarządzalny (1 sztuka)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Charakterystyka (wymagania minimalne)** |
| **1.1** | **Architektura portów** | Gigabit Ethernet |
| **1.2** | **Typ przełącznika** | Zarządzalny |
| **1.3** | **Warstwa przełącznika** | L3 |
| **1.4** | **Prędkość magistrali** | 176 Gb/s |
| **1.5** | **Przepustowość** | 130.9 Mp/s |
| **1.6** | **Bufor pamięci** | 16 MB |
| **1.7** | **Rozmiar tablicy adresów MAC** | 16 tys. |
| **1.8** | **Warstwa przełączania** | 2 |
| **1.9** | **Całkowita ilość portów** | 52 |
| **1.10** | **Ilość złącz 10/100** | Brak |
| **1.11** | **Ilość złącz 10/100/1000** | 48 |
| **1.12** | **Ilość złącz 100/1000/10000** | 2 |
| **1.13** | **Ilość złącz SFP** | 2 |
| **1.14** | **Złącza PoE/PoE+** | Nie |
| **1.15** | **Rodzaj obudowy** | Rack |
| **1.16** | **Szerokość [mm]** | 440 |
| **1.17** | **Wysokość [mm]** | 44 |
| **1.18** | **Głębokość [mm]** | 310 |

**2. System zabezpieczenia danych przed wyciekiem informacji.**

Wymaga się dostawy kompletnego rozwiązania do ochrony stacji roboczych Windows przed wyciekiem danych, pochodzącego od jednego producenta, o minimalnej funkcjonalności opisanej poniżej. Wymagane jest, aby cała funkcjonalność była dostępna w ramach jednej, jednolitej instalacji oferowanego systemu ochrony danych przed wyciekiem ze zintegrowanym systemem kontroli portów i szyfrowaniem – całość realizowana w ramach jednego agenta na stacjach roboczych.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Charakterystyka (wymagania minimalne)** |
| **2.1** | **Wymagania ogólne** | Rozwiązanie ma chronić dane na stacjach roboczych Windows przed wyciekiem, poprzez kontrolę portów fizycznych i podłączanych do nich nośników zewnętrznych oraz przez szyfrowanie danych na dyskach lokalnych i nośnikach zewnętrznych.  Rozwiązanie powinno działać w oparciu o definiowanie polityk bezpieczeństwa i integrować się z Active Directory przez wiązanie polityk bezpieczeństwa z obiektami Active Directory. Wymaga się, aby polityka mogła być powiązania z różnymi rodzajami obiektów AD:   * Domena * Jednostka Organizacyjna (OU) * Grupa * Użytkownik * Komputer   Rozwiązanie nie może w żaden sposób modyfikować, usuwać ani tworzyć obiektów w drzewie AD.  Rozwiązanie powinno składać się z pojedynczego serwera zarządzającego, oferującego konsolę administracyjną do zarządzania politykami bezpieczeństwa, konfigurowania i monitorowania pracy systemu oraz z agenta, instalowanego na stacjach roboczych, który egzekwuje polityki bezpieczeństwa przypisane do komputera bądź użytkownika.  Dystrybucja polityk bezpieczeństwa i ich odświeżanie na stacjach roboczych muszą zachodzić automatycznie i cyklicznie z częstotliwością definiowaną przez administratora, ale również z możliwością wymuszonego odświeżenia na żądanie z poziomu konsoli administracyjnej oraz ze stacji roboczej.  Wymaga się, aby polityki bezpieczeństwa były egzekwowane również w trybie „offline”, czyli gdy stacja robocza nie ma kontaktu z serwerem zarządzającym (np. laptop poza firmą).  Wymagane jest dostarczenie pliku instalacyjnego agenta w postaci pakietu MSI, z możliwością dystrybucji tego pakietu co najmniej przez Active Directory GPO lub inne systemy dystrybucji centralnej oprogramowania.  Agent musi być wspierany dla stacji roboczych z biznesową wersją Windows 10/11. |
| **2.2** | **Kontrola portów fizycznych i nośników zewnętrznych** | Produkt musi umożliwiać całkowite blokowanie użycia portów fizycznych:   * USB * Firewire * PCMCIA * Secure Digital * Serial * Paralel * Porty wewnętrzne * WiFi * Bluetooth   Wymagane jest, aby produkt identyfikował i raportował urządzenia podłączane do portów USB stacji roboczych, według typu, producenta, modelu i numeru seryjnego. Funkcja ta jest konieczna, by usprawnić proces definiowania polityk bezpieczeństwa, dotyczących kontroli nośników zewnętrznych. Niezbędna jest możliwość zdalnego przeskanowania stacji roboczych z poziomu konsoli zarządzającej w celu zidentyfikowania podłączanych do nich urządzeń zewnętrznych.  Produkt musi umożliwiać blokowanie wybranych typów urządzeń podłączanych do portu USB, rozróżniając:   * Telefony komórkowe * Urządzenia oparte o system Android * Urządzenia oparte o system iOS * Urządzenia PDA * Smart Card * Urządzenia drukujące * Adaptery sieciowe * Urządzenia audio/video * Urządzenia interfejsu HID * Urządzenia do przetwarzania obrazów * Sprzętowe KeyLoggery   Produkt musi posiadać funkcję definiowania “białych list”, czyli urządzeń wyjątkowo dopuszczonych do podłączenia, identyfikowanych przez określenie producenta, modelu i numeru seryjnego urządzenia.  Dla zewnętrznych urządzeń pamięci masowej typu: pendrive, napędy CD/DVD, zewnętrzne dyski twarde – musi być możliwość zdefiniowania w polityce bezpieczeństwa mechanizmów:   * Blokowanie urządzeń danego typu * Korzystanie w trybie „tylko do odczytu” * Wymuszenie szyfrowania danych na nośniku * Blokowanie możliwości odczytu z nośnika plików określonego typu (np. plików wykonywalnych) * Blokowanie możliwości zapisywania na nośniku plików określonego typu * Rejestrowanie w logach wszystkich zapisów i odczytów z nośnika, również wtedy, gdy stacja pracuje „offline”   Szyfrowanie danych na nośnikach zewnętrznych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Musi być możliwość zapisania i odczytania danych z zaszyfrowanego nośnika na dowolnej stacji roboczej wyposażonej w agenta oferowanego rozwiązania. |
| **2.3** | **Szyfrowanie dysku lokalnego** | Wymaga się funkcjonalności szyfrowania danych na dysku lokalnym, inicjowanej tym samym jednolitym mechanizmem, co inne funkcjonalności, tj. przez przypisanie odpowiedniej polityki bezpieczeństwa do stacji roboczej.  Wymagane jest, aby szyfrowaniem objęte były tylko dane użytkowników, bez szyfrowania sektora rozruchowego i plików systemowych Windows. Przypisanie polityki szyfrowania do stacji roboczej powinno spowodować zaszyfrowanie danych na dysku.  Szyfrowanie danych na dyskach lokalnych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Proces deszyfrowania/szyfrowania musi być realizowany w czasie rzeczywistym przy modyfikacji plików przez użytkownika.  Obsługa szyfrowania musi być realizowana w całości przez agenta oferowanego rozwiązania, bez konieczności korzystania z rozwiązań zewnętrznych.  Wymaga się, aby zaszyfrowane dane były dostępne dla każdego użytkownika, który na stacji roboczej poprawnie zaloguje się na swoje konto domenowe (w zakresie jego uprawnień na poziomie systemu plików).  Wymaga się, aby żadne zaszyfrowane dane nie były dostępne, gdy na stacji roboczej zaloguje się pracownik Helpdesku. Umożliwi to udzielanie wsparcia użytkownikom w zakresie utrzymania systemu operacyjnego, bez ryzyka ujawnienia treści ich danych przechowywanych na stacji roboczej.  Musi być dostępne narzędzie, pozwalające na odszyfrowanie danych z dysku w przypadku, gdy nie da się uruchomić stacji roboczej w normalnym trybie, np. na skutek uszkodzenia systemu operacyjnego. Skorzystanie z narzędzia musi wymagać akceptacji administratora systemu, np. poprzez wygenerowanie jednorazowego kodu/hasła. |
| **2.4** | **Pozostałe wymagania** | Wymaga się, by produkt zaopatrzony był w funkcje zabezpieczające przed próbami ingerencji użytkowników w działanie agenta:   * Odinstalowanie oprogramowania możliwe dzięki hasłu, które zna wyłącznie administrator IT * Ochrona przed użytkownikami posiadającymi uprawnienia administratora, chcącymi usunąć bądź wyłączyć oprogramowanie * Rejestrowanie wszelkich prób manipulacji przez użytkowników (łącznie z usuwaniem logów) * Wszystkie pliki logów muszą być zaszyfrowane przed nieautoryzowanym dostępem i próbą skasowania * Wszystkie połączenia między aplikacją agencką na stacji roboczej a serwerem zarządzającym muszą być zaszyfrowane przy użyciu protokołu SSL   Musi istnieć możliwość czasowego wstrzymania (zawieszenia) ochrony na stacji roboczej, bez konieczności modyfikacji lub usuwania i ponownego przypisywania polityk bezpieczeństwa. Wstrzymanie ochrony musi wymagać akceptacji administratora systemu, np. przez wygenerowanie jednorazowego hasła.  W czasie swojego działania agent na stacji roboczej nie może obciążać zasobów (CPU, RAM, dysk) w stopniu odczuwalnym przez użytkownika i utrudniającym normalną pracę. Dopuszczalne jest większe obciążenie stacji jedynie przy pierwszym szyfrowaniu dysku lokalnego.  Powinna być możliwość zdefiniowania własnej treści komunikatów w języku polskim, wyświetlanych przez agenta na stacji roboczej.  Wymagana jest możliwość instalacji agenta w trybie ukrytym, tj. bez widoczności żadnych ikonek i bez wyświetlania jakichkolwiek komunikatów na stacji roboczej.  Rozwiązanie musi posiadać wbudowany mechanizm automatycznego wykonywania backupu swojej konfiguracji i zgromadzonych logów wg harmonogramu zdefiniowanego przez administratora. System musi umożliwiać całkowite odtworzenie serwera zarządzającego z takiego backupu na wypadek awarii, bez konieczności reinstalowania agentów.  Proponowane rozwiązanie musi wspierać instalację na wirtualnej platformie VMware lub Hyper-V i być z nią kompatybilne.  Rozwiązanie musi być uruchomione na wskazanych zasobach Zamawiającego i nie może wymagać żadnych dodatkowych zewnętrznych komponentów, np. zewnętrznych baz danych lub zewnętrznych programów szyfrujących.  Rozwiązanie musi obsłużyć minimum 70 stacji roboczych.  Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej z odnawianym corocznie supportem, zawierającym wsparcie techniczne producenta oraz dostęp do poprawek i nowych wersji.  Wymaga się, aby funkcjonalność szyfrowania dysków lokalnych była licencjonowana osobno od funkcjonalności kontroli portów fizycznych i nośników zewnętrznych, pozwalając na elastyczność w doborze licencji do potrzeb.  Wymaga się dostarczenia 70 licencji wieczystych z 18 miesięcznym wsparciem technicznym dla funkcjonalności kontroli portów fizycznych i nośników zewnętrznych oraz 70 licencji wieczystych z 18 miesięcznym wsparciem technicznym dla funkcjonalności szyfrowania dysków lokalnych. |
| **2.5** | **Usługi** | Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalifikowanego inżyniera, certyfikowanego przez producenta rozwiązania:  - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego  - szkolenie dla administratora rozwiązania  - wsparcie w języku polskim w trybie 8x5 w dni robocze  - kwartalny przegląd konfiguracji rozwiązania  Wymaga się, aby dostawca przedstawił:  - oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia  - osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie |

**3. Urządzenie z systemem do ochrony poczty elektronicznej (1 sztuka)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Charakterystyka (wymagania minimalne)** |
| **3.1** | **Wymagania ogólne** | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.  Dopuszcza się aby poszczególne elementy wchodzące w skład systemu 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.  Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.  Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:   1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). |
| **3.2** | **Parametry fizyczne systemu antyspamowego** | 1. System musi być wyposażony w interfejsy:  * 4 porty Gigabit Ethernet RJ-45.  1. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB . 2. System musi posiadać wbudowany port konsoli szeregowej. 3. Zasilanie z sieci 230V/50Hz. |
| **3.3** | **Ogólne funkcje systemu ochrony poczty** | Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:   1. Wsparcie dla co najmniej 20 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |
| **3.4** | **Kontrola antywirusowa i ochrona przed malware** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake. |
| **3.5** | **Kontrola antyspamowa** | System musi zapewniać poniższe funkcje i metody filtrowania spamu:   1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |
| **3.6** | **Ochrona przed atakami na usługę poczty** | System musi zapewniać poniższe funkcje i metody filtrowania:   1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy. |
| **3.7** | **Funkcje logowania i raportowania** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu. |
| **3.8** | **Funkcje pracy w trybie wysokiej dostępności (HA)** | System ochrony poczty musi zapewniać poniższe funkcje: Aktualizacje sygnatur, dostęp do bazy spamu |
| **3.9** | **Aktualizacje sygnatur, dostęp do bazy spamu** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:   1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |
| **3.10** | **Zarządzanie** | System ochrony poczty musi zapewniać poniższe funkcje:   1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. |
| **3.11** | **Certyfikaty** | Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:   1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified. |
| **3.12** | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:   1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 18 miesięcy. |
| **3.13** | **Gwarancja oraz wsparcie** | 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 18 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **3.14** | **Rozszerzone wsparcie serwisowe** | 1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 18 miesięcy.   Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polski 24x7. Oferent winien przedłożyć dokumenty:   * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego. |
| **3.15** | **Wdrożenie + szkolenie** | 1. Wdrożenie + konfiguracja urządzenia. Jednodniowe (8h) certyfikowane szkolenie dla 1 administratora w siedzibie zamawiającego. |
| **3.16** | **Opisy do wymagań ogólnych** | 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |

**4. System kontroli i zarządzania dostępem do sieci (System NAC)**

Przedmiotem jest dostarczenie centralnego systemu kontroli i zarządzania dostępem do sieci LAN oraz WLAN współpracującego z posiadaną przez Zamawiającego infrastrukturą dostępową.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu NAC były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: Vmware vSphere oraz Microsoft Hyper-V.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Parametry** | **Charakterystyka (wymagania minimalne)** |
| **4.1** | **Architektura** | 1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości stopniowego zwiększania wydajności systemu (skalowanie). 2. Elementy Systemu muszą umożliwiać klastrowanie active-passive. 3. System NAC musi pracować w trybie out-of-band, tj. realizować wszystkie wymagane funkcje bez konieczności analizy ruchu sieciowego (na porcie SPAN, inline). 4. Wszystkie elementy Sytemu powinny być zarządzane centralnie. 5. System i jego wszystkie funkcje muszą w pełni współpracować z urządzeniami dostarczonymi w ramach tego postępowania. |
| **4.2** | **Funkcje Systemu** | 1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:    * standardu 802.1X    * adresu MAC urządzenia    * formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie. 2. System musi obsługiwać uwierzytelnianie w oparciu o:   wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń.   1. System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS. 2. System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci. 3. System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje:    * adresy MAC przełączników, urządzeń końcowych i dostępowych,    * adresy IP ww. urządzeń    * identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe    * stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena. w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów    * informacje o użytkownikach    * nazwa użytkownika do którego przypisany jest urządzenie końcowe    * nazwa zalogowego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja    * profil/rola jak została przydzielona urządzeniowi końcowemu przez System    * data zarejestrowania urządzenia końcowego w Systemie    * data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia 4. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) opartych o złożone i wielowarunkowe polityki bezpieczeństwa. Powinny one obejmować co najmniej: lokalizacja urządzenia w sieci, przynależność do grupy administracyjnej, parametr opisujący urządzenie lub użytkownika. 5. System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny oraz blokowania. 6. System musi zapewniać możliwość powiadamiania poprzez SYSLOG oraz pocztę elektroniczną o sytuacjach krytycznych np. związanych z próbą nieautoryzowanego dostępu do sieci lub awarii wewnętrznych usług Systemu NAC. 7. System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API. 8. System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji. 9. System musi posiadać bazę minimum 30 kategorii urządzeń końcowych. 10. System musi mieć możliwość klasyfikacji jednorazowej przy wstępnym uwierzytelnianiu/rejestracji bądź klasyfikacji wielokrotnej. Klasyfikacja urządzeń i użytkowników musi bazować na harmonogramie z częstotliwością w przedziale od kilku minut do kilku tygodni. 11. System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa. 12. System musi obsługiwać telefony IP wraz z możliwością podłączenia do nich stacji końcowych (przez wbudowany przełącznik w telefonie) przypisując każdemu z urządzeń dedykowane polityki bezpieczeństwa. 13. System musi podejmować decyzję o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta. 14. Klasyfikacja urządzeń końcowych z użyciem agenta dedykowanego dla komputerów z systemem Windows i MAC OS X musi umożliwiać przeprowadzenie następujących testów:     1. Sprawdzenie wersji agenta     2. Sprawdzenie wersji systemu operacyjnego,     3. Sprawdzenie obecności i stanu oprogramowania antywirusowego (niezainstalowany/zainstalowany, uruchomiona ochrona, zaktualizowany),     4. test zapory (włączona/wyłączona),     5. test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),     6. test usługi Windows Update z opcją automatycznego naprawienia niezgodności     7. test obecności/niewystępowania pliku o określonej nazwie     8. test obecności procesu (uruchomiony /nieuruchomiony)     9. test rejestru dla systemów Windows (obecność klucza o zdefiniowanej nazwie, typie wartości i wartości, równy bądź różny zadanemu)     10. test stanu usługi (uruchomiona/nieuruchomiona)     11. test obecności aplikacji (sprawdzenie czy aplikacja zdefiniowanej nazwie jest zainstalowana) 15. Wykorzystywany przez system Agent nie może wprowadzać zmian w działaniu aplikacji lub procesów systemu operacyjnego. 16. System musi mieć możliwość przeprowadzania różnych metod testowania w zależności od lokalizacji urządzenia w sieci, przynależności do grupy administracyjnej, parametru opisującego urządzenie lub użytkownika. 17. Podczas oceniania urządzenia końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów w przypadku braku zgodności. 18. System musi mieć możliwość przeniesienia urządzenia do kwarantanny w przypadku braku komunikacji z agentem. 19. Na urządzeniu podlegającym kwarantannie musi zostać wyświetlona informacja o fakcie przeniesienia urządzenia do kwarantanny oraz informacja z wytycznymi o działaniach jakie użytkownik urządzenia musi podjąć w celu usunięcia niezgodności. 20. Administrator musi mieć możliwość określenia poziomu niezgodności z politykami, po którym będzie następowało przeniesienia stacji do kwarantanny. 21. System musi zapewniać integrację z rozwiązaniami bezpieczeństwa (platformy Firewall, systemy SIEM, systemy Antymalware, systemy MDM) na potrzeby oceny stanu urządzeń końcowych oraz określenia ich zgodności z polityką bezpieczeństwa NAC. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect” przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci. 22. System musi zapewniać integrację z platformami typu Firewall/SIEM w ramach której:     1. w przypadku wykrycia zagrożenia przez system Firewall/SIEM (np. wirus, malware) i przesłania takiej informacji do systemu NAC mogą zostać podjęte następujące akcje automatyczne:        * powiadomienie administratora o zdarzeniu.        * oznaczenie urządzenia końcowego jako potencjalnie niebezpiecznego „z ryzykiem”.        * zablokowanie dostępu do sieci.        * przeniesienie urządzenia do kwarantanny.     2. System NAC - po udzieleniu stacji roboczej dostępu do sieci – przekazuje do systemu Firewall kontekst użytkownika, który jest zalogowany na tym urządzeniu. 23. System musi zapewniać integrację z platformami typu Firewall w ramach której:     1. możliwy jest import stanu sesji urządzeń końcowych z platformy Firewall i wykorzystanie tych informacji jako danych wejściowych w konfiguracji metod profilowania urządzeń końcowych.     2. możliwe jest wykorzystanie funkcji rozpoznawania urządzeń końcowych przez platformę Firewall jako daną wejściową w konfiguracji metod profilowania urządzeń końcowych. 24. System musi zapewniać integrację z serwerem wdrażania, zarządzania, rejestrowania i monitorowania urządzeń końcowych w ramach której:     1. System NAC może gromadzić dane o urządzeniach końcowych (nazwa urządzenia końcowego, typ, system operacyjny, użytkownik, zgodność z polityką bezpieczeństwa)     2. System NAC może wykorzystać zgromadzone dane do rejestracji urządzenia końcowego. |
| **4.3** | **Profilowanie urządzeń** | 1. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic. 2. System musi posiadać funkcję automatycznego profilowania urządzeń nie posiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci. 3. System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych. 4. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. 5. System musi rozpoznawać co najmniej następujące rodzaje urządzeń:    * urządzenia z systemem Android,    * urządzenia Apple (iPad, iPhone, iPod )    * drukarki sieciowe,    * telefony IP,    * stacje robocza z systemem Microsoft Windows,    * stacje robocza z systemem MAC OS,    * stacje robocza z systemem Linux. 6. System musi posiadać funkcję wykrywanie nieautoryzowanych serwerów DHCP. 7. System musi posiadać funkcję wykrywania procesu NAT na urządzeniach końcowych. |
| **4.4** | **Logowanie, Raportowanie i Alarmowanie** | 1. System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń). 2. System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego. 3. System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie. 4. System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych. 5. System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy. 6. System musi oferować możliwość tworzenia własnych szablonów raportów. 7. System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog. 8. System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora. 9. System musi umożliwiać przekazywanie informacji do systemów zewnętrznych poprzez mechanizm np. ODBC. 10. System NAC musi zapewniać integrację z modułem analizy i raportowania pochodzącym od tego samego producenta, w którym możliwe jest – oprócz logowania i raportowania – tworzenie reguł korelujących i alarmujących. |
| **4.5** | **Zarządzanie systemem** | 1. System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową w wersji oferowanej przez producenta przeglądarki lub dedykowaną aplikację. 2. System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników lub zewnętrzne repozytorium użytkowników (LDAP lub Radius). 3. System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania - RBA. 4. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do poszczególnych elementów systemu. 5. System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę koloru tła i czcionek, treści, grafiki. 6. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych. |
| **4.6** | **Zarządzanie dostępem gościnnym** | 1. System musi umożliwiać przyznawanie dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez wypełnienie formularza w portalu rejestracyjnym. 2. System musi umożliwiać realizację usług BYOD dla urządzeń prywatnych pracowników. 3. Funkcja portalu rejestracyjnego powinna działać bez udziału lub przy minimalnym udziale pracowników IT. System powinien posiadać możliwość delegowania uprawnień do akceptowania kont gości przez pracowników nieposiadających uprawnień administracyjnych w Systemie. 4. Wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego. 5. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych. 6. System musi umożliwiać przyznanie dostępu czasowego dla gości. 7. System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki. |
| **4.7** | **Licencje i serwisy** | 1. W ramach postępowania koniecznym jest dostarczenie 100 licencji umożliwiających uruchomienie wszystkich wyżej wymienionych funkcji z zastosowaniem agenta na stacjach końcowych, z założeniem że są one równocześnie podłączone do sieci lokalnej LAN i sieci bezprzewodowej WLAN. 2. Licencje w ramach rozwiązania powinny być dostarczone w modelu permanentnym. Zamawiający nie dopuszcza licencji bazujących na subskrypcji. 3. Dostarczone elementy systemu NAC muszą zawierać wszystkie niezbędne komponenty programowe, na których możliwa będzie licencyjna rozbudowa do min. 100 urządzeń równocześnie podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN, z uwzględnieniem instalacji agentowej. 4. Wsparcie: elementy systemu muszą być objęte serwisem producenta przez okres 18 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. 5. Elementy systemu muszą być dostarczone w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. |
| **4.8** | **Opisy do wymagań ogólnych** | 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |
| **4.9** | **Zakres wdrożenia:** | 1. Zamawiający wymaga wdrożenia najnowszej, dostępnej wersji systemu NAC oferowanej przez producenta systemu. 2. Przygotowanie i wdrożenie polityk kontroli dostępu, które zostaną uzgodnione z Zamawiającym. 3. Przygotowanie projektu wdrożenia wraz z harmonogramem, który musi zostać zaakceptowany przez Zamawiającego. 4. Zamawiający wymaga wdrożenia/implementacji oferowanego sytemu NAC w środowisku Zamawiającego w tym konfiguracja urządzeń we wskazanych lokalizacjach, testów funkcjonalnych oraz dokumentacji powykonawczej. 5. Zasilenie inicjalne Systemu informacjami o urządzeniach objętych wdrożeniem, dostarczonych przez Zamawiającego. 6. Sporządzenie instrukcji konfiguracji przełączników sieciowe, urządzeń UTM i kontrolera WLC, wymaganej do współpracy z Systemem. 7. Przygotowanie procedur awaryjnych. 8. Zamawiający wymaga, aby wraz z System oraz kontraktem serwisowym oferta obejmowała minimum 1 dniowy instruktaż powdrożeniowy dla 1 pracownika Zamawiającego oraz certyfikowane warsztaty dla 2 pracowników Zamawiającego obejmujące zakresem obsługę Systemu NAC. Warsztaty muszą być przeprowadzone w siedzibie Zamawiającego w języku polskim. |

**5. System SIEM do zbierania i analizy logów.**

# **Minimalne wymagania systemu:**

* System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
* System musi pracować w oparciu o architekturę Linux.
* System musi mieć możliwość centralnego zbierania i zarządzania logami
* System działać w trybie zbliżonym do rzeczywistego
* System musi umożliwiać funkcjonowanie bez dostępu do sieci internet
* System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
* Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
* System musi zapewniać efektywną obsługę do 20 GB danych dziennie
* System musi zapewniać retencję danych w okresie minimum 365 dni.
* Oferowany system nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
* Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
* System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
* Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
* Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
* Interfejs musi posiadać angielską lub polską wersję językową.
* System musi być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
* System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
* System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
* System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
* System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
* System musi pozwalać na tworzenie parserów z poziomu GUI
* System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
* System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
* System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
* Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent\_bytes), rozmiar pliku (file\_size) i czas trwania sesji (session\_duration).
* Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.
* Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
* Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
* Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
* Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
* System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
* System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
* Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
* System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
* System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
* Syslog,
* WEF,
* Flat file,
* Event log,
* WMI,
* SNMP trap,
* XML,
* JSON,
* JDBC/ODBC
* CSV,
* Email,
* Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
* System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
* System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka
* System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
* System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
* Operacja z rekordami bazy danych musza być wykonywane jedynie za pomocą składni JSON z wykorzystaniem udokumentowanego API.
* Wykorzystanie bazy danych musi odbywać się za pomocą REST API z pominięciem wykorzystania klienta typu SQL client.
* System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
* Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
* System musi posiadać predefiniowany zestaw parserów zdarzeń.
* System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta.
* System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
* System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
* System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
* Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
* Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
* System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
* System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
* System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w Systemie danych.
* Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
* System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.
* System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
* Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
* System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL oraz Piped Processing Language (PPL).
* System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
* System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
* System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
* Wykrycia dowolnej treści w logach,
* Wykrycia wystąpienia wartości pola na wybranej liście,
* Wykrycia niewystępowania wartości pola na wybranej liście,
* Wykrycia zmiany jednego z kilku pól,
* Wykrycia zdarzeń występujących z zadaną częstotliwością,
* Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
* Wykrycia zaniku Wiadomości,
* Wykrycia nowej wartości pola w zadanym okresie czasu,
* Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
* System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
* Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
* System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
* System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.
* System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
* System musi umożliwiać analizę ruchu sieciowego poprzez przechwytywanie i inspekcję pakietów w czasie rzeczywistym, w tym minimum protokołów HTTP DNS, FTP oraz SSH.
* System na bazie gromadzonej kopii ruchu sieciowego musi identyfikować i klasyfikować ataki w oparciu o sygnatury oraz zachowanie użytkowników.
* System musi umożliwiać zapisywanie pakietów ruchu sieciowego w formacie PCAP.
* System musi umożliwiać gromadzenie i analizowanie danych Netflow, w tym: IPFIX, sFlow, J-Flow, Netflow v9.
* System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
* System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
* System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
* Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
* System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
* Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
* System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
* System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
* System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
* Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
* System musi posiadać wbudowany, dostepny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
* System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 18 miesięcy.
* Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
* System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
* Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostepnej stronie internetowej producenta.
* Zamawiający oczekuje, że Wykonawca wraz z licencją produkcyjną Wykonawca zobligowany jest dostarczyć licencję na potrzeby środowiska testowego, która umożliwi przetwarzanie minimum 1000 EPS.
* Licencja testowa musi być objęta supportem producenta na takich samych zasadach jak licencja produkcyjna.

**Dostęp do systemu**

* Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywac się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.
* Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protoków TLS w wersji minimum 1.3.
* System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
* Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
* Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP,Radius
* Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
* System musi wspierać mechanizm logowania typu Single Sign On.
* System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
* System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
* System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.

**Przyjmowanie, identyfikacja i wizualizacja danych**

* Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
* System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
* System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.
* System posiada natywną integrację z Mitre ATT@CK

**Reguły korelacyjne, alerty i obsługa incydentów**

* System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
* System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
* System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
* System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST, ISO 27001
* System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit’u i wykrywania ukrytych procesów, plików, portów
* System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
* System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

**Raportowanie i Archiwizacja danych**

* System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
* Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
* Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
* Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
* System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
* Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
* System musi generować raporty do formatów minimum PDF, docx oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.

**Zakres oczekiwanych prac związanych z wdrożenie systemu:**

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

**Szkolenia**

* Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem dla 1 pracownika zamawiającego w wymiarze 2 dni roboczych (min. 16h roboczych).
* Grupa szkoleniowa będzie miała nie więcej niż 10 słuchaczy.
* Szkolenie odbędzie się w siedzibie Zamawiającego.
* Szkolenie musi być prowadzone w języku polskim.
* Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
* Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.

**Utrzymanie systemu**

* Usługi utrzymania systemu oferowane przez producenta muszą być potwierdzone certyfikacją wg. normy ISO 27001:2017
* Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostepnej stronie internetowej producenta.

**Integracja z SOAR**

* Producent systemu SIEM musi umożliwiać rozbudowę oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewnić gotową integrację z systemem SOAR tego samego producenta

**6. Wznowienie licencji fizycznego UTM.**

Zakup licencji dla posiadanego urządzenia Watchguard Firebox M270 Total Security Suite na okres 24 miesięcy.