**Załącznik nr 1 – Szczegółowy Opis Przedmiotu Zamówienia**

**Znak: OR.271.4.2025.RS**

**Dotyczy:** postępowania o udzielenie zamówienia publicznego pn. „**Dostawa urządzeń   
i oprogramowania zwiększających odporność na cyberataki wraz z wdrożeniem w ramach realizacji projektu „Cyberbezpieczna Gmina Suchedniów”\_2**

**Wykaz:**

**Dostawa sprzętu informatycznego oraz oprogramowania:**

* Specjalistyczne wsparcie IT - usługa wsparcia trwać będzie   
  nie dłużej jak do 14 czerwca 2026 r. 14 szt.
* Centralny System Bezpieczeństwa 1 szt.
* Oprogramowanie do wykonywania kopii zapasowych wraz z 1 szt.
  + Certyfikowane, stacjonarne szkolenie z obsługi   
    systemu do Back-up danych 1 szt.
* Bezpieczne logowanie wraz z 1 szt.
  + Certyfikowane szkolenie z zarządzania   
    Active Directory 1 szt.
* Switch zarządzalny 1 szt.
* UPS - stanowiskowy 30 szt.
* UTM wraz z 3 szt.
  + Certyfikowane szkolenie z urządzeń klasy UTM 1 szt.
* Serwer - na potrzeby CSB 1 szt.
* System operacyjny do serwera 1 szt.
* Licencje dostępowe do serwera 60 szt.
* NAS – Network Attached Storage 1 szt.
* UPS 1 szt.

**Specjalistyczne wsparcie IT - usługa wsparcia trwać będzie nie dłużej jak do 14 czerwca 2026 r.**

W ramach zadania obowiązkiem Wykonawcy będzie świadczenie specjalistycznego wsparcia IT   
w zakresie cyberbezpieczeństwa. Wnioskodawca w ramach każdej z zaoferowanych paczek roboczogodzin będzie świadczył specjalistyczne wsparcie IT w wymiarze 8h stacjonarnie, 30h online w następującym zakresie:

1. Wdrożenie reguł zgodności z przepisami prawnymi oraz standardami bezpieczeństwa.
2. Konfiguracja i zarządzanie firewallami, IDS/IPS i innymi mechanizmami obronnymi.
3. Zarządzanie dostępem i autoryzacją użytkowników.
4. Monitoring sieci i alarmowanie w czasie rzeczywistym.
5. Wdrożenie (na zlecenie) reguł dla Backupu i archiwizacji danych.
6. Szyfrowanie danych wrażliwych.
7. Zabezpieczenie przed oprogramowaniem złośliwym – konfiguracja: antywirus, antimalware.
8. Opracowanie i implementacja planu reagowania na incydenty bezpieczeństwa.
9. Analiza po incydentach i rekomendacje.
10. Stałe monitorowanie logów i zdarzeń związanych z bezpieczeństwem.
11. Zlecone raporty dotyczące stanu bezpieczeństwa.
12. Reagowanie na zgłoszone incydenty związane z bezpieczeństwem
13. Wsparcie w obsłudze wdrażonego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM.

Wszystkie zapisy rozumiane jako doradztwo i konfiguracja urządzeń oraz systemów zakupionych   
w ramach projektu będą realizowane zgodnie z założonymi incydentami. Incydenty będą mogły być zakładane przez Zamawiającego poprzez udostępnione przez Wykonawcę kanały komunikacji, takie jak co najmniej:

* Strona www (24h na dobę)
* Adres email (24h na dobę)
* Telefon w dni robocze (7:30 – 15:30) – infolinia w języku polskim.

Dla wsparcia stacjonarnego, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/3) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 3 dni roboczych na realizację. Dla wsparcia online, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/2) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 1 dzień robocze na realizację.

WSPARCIE STACJONARNE 8h w ramach paczki godzin:

W przypadku usług wykonywanych stacjonarnie, po zgłoszeniu przez Zamawiającego incydentu - konieczności wizyty stacjonarnej w Urzędzie, Wykonawca ma 3 dni robocze na realizację tego zadania. Wykonawca musi zaanonsować dzień swojej wizyty w Jednostce Zamawiającego w ramach czasu wskazanego na reakcję (1 dzień roboczy).

Wezwanie Wykonawcy do świadczenia usługi stacjonarnej odbywać będzie się maksymalnie w ramach dwóch wizyt w ramach jednej paczki godzin.

Każda wizyta i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać   
się z wykorzystaniem systemu informatycznego lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego.

WSPARCIE ONLINE 30h w ramach paczki godzin:

W przypadku usług wykonywanych online, po zgłoszeniu przez Zamawiającego incydentu - konieczności wsparcia online, Wykonawca ma 1 dzień robocze na realizację tego zadania (1 dzień roboczy, następujący po dniu przeznaczonym na reakcje). Wykonawca musi zaanonsować termin wykonywanych prac w ramach czasu wskazanego na reakcję (1 dzień roboczy).

Wezwanie Wykonawcy do świadczenia usługi wsparcia online odbywać będzie się maksymalnie w ramach 5 zleceń w ramach jednej paczki. Każda usługa wsparcia online i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego.

Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Podpisane protokoły będą podstawą do wystawienia faktur (zgodnie z umową).

Dla zgłoszeń obu typów incydentów Zamawiający przekaże wykonawcy imienną listę osób uprawnionych do zgłaszania i raportowania incydentów (maksymalnie 3 osoby).

WYKORZYSTANIE PACZEK GODZIN:

W ramach zadania, Wykonawca świadczy na rzecz Zamawiającego usługę specjalistycznego wsparcia IT w 14 paczkach godzin w wymiarze 8h stacjonarnie, 30h online (dalej paczka godzin), a także pozostaje w trybie gotowości do podjęcia ww. zleceń w okresie o mniejszej intensyfikacji zgłoszeń.

* Specjalistyczne wsparcie IT świadczone będzie od dnia podpisania umowy.
* Wykonawca przez cały okres świadczenia usługi utrzymuje stan gotowości, do realizacji zleceń – incydentów na rzecz zamawiającego.
* Paczka godzin, będzie wykorzystana maksymalnie w ciągu 30 dni.
* Okres 30 dni stanowi okres rozliczeniowy dla każdej kolejnej paczki godzin, rozpoczynając od dnia podpisania umowy. Kolejne okresy rozliczeniowe będą liczone od dnia wykorzystania paczki godzin, lub upływie 30 dni.
* Zamawiający w okresie 30 dni może wykorzystać maksymalnie 2 paczki godzin. Wykorzystanie większej ilości wsparcia – paczek godzin, może odbyć się tylko za obopólną zgodą Zmawiającego   
  i Wykonawcy.
* Wykorzystanie paczki godzin, klasyfikowane będzie zawsze dla okresu, w którym Zamawiający przekazał zgłoszenie incydentu, także w przypadkach, kiedy Wykonawca w jego obsłudze wyszedł poza okres trwania paczki godzin (np. zgłoszenie przekazane w 29 dniu okresu rozliczeniowego pierwszej paczki godzin, obsłużone w 32 dniu będzie zaliczane dla pierwszej paczki godzin).
* W przypadku niewykorzystania wszystkich godzin (stacjonarnych, lub online) w ciągu 30 dni,   
  w ramach jednej paczki godzin niewykorzystane godziny nie przechodzą na kolejny okres. Nie zmienia to wynagrodzenia Wykonawcy, pod warunkiem pozostania w gotowości do wykonania zleceń incydentów na rzecz Zamawiającego.
* Jeżeli Zamawiający wykorzysta jeden typ wsparcia (godziny stacjonarne, lub online) może wymienić typ wsparcia według przelicznika: 1 godzina stacjonarna = 6 godzin online.

**Centralny System Bezpieczeństwa: Oprogramowanie klasy SIEM**

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową. Oprogramowanie musi posiadać wsparcie do dnia 14-06-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta. Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

* Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.
* Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.
* Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.
* Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).
* Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.
* Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.
* Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.
* Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.
* Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.
* Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.
* Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).
* Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.
* Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.
* Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.
* Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA. Cały interfejs użytkownika powinien być́ dostosowany pod aktualne wymagania prawne związane z dostępnością̨ serwisów użyteczności publicznej dla osób z niepełnosprawnościami. Na podstawie uzyskanych efektów serwis będzie mógł być́ udostępniony publicznie. Treści multimedialne muszą być́ dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą̨ być́ z przyczyn technicznych tak zbudowane, by uczynić́ je dostępnymi dla wszystkich użytkowników muszą posiadać́ alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.
* Zgodność́ ze standardami HTML i CSS całego serwisu www.
* Kontrast kolorystyczny między tłem, a tekstem musi być́ zgodny z zaleceniami WCAG 2.1 AA.
* System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.
* System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

MODUŁ ANALIZY PODATNOŚCI

1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.

Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności “nowe”, których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

1.2.  Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

1.3.  Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

MODUŁ MONITORINGU ZASOBÓW

2.1.  Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

2.2.  Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami

System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

2.3.  Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach

System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów

Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko “nowe” problemy i zdarzenia oraz te, których status nie został zmieniony na “rozwiązany” bądź “anulowany”. Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, system przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: “help-desk”, przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej

Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT

System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT

System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.8 Zdalny dostęp do urządzeń końcowych

System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.

2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych

System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować   
co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie   
i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.

2.10 Analiza ruchu sieciowego

System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.

2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach

System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto   
w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

MODUŁ ANALIZY LOGÓW

3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

3.2. Możliwość analizy tzw. „customowych” logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.

System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania,   
a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. “customowych” logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.

3.3.  Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania   
(w szczególności oprogramowania dziedzinowego - “customlogów”), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

3.4. Przegląd i analiza logów dotyczących działań użytkowników.

W module analizy logów muszą być agregowane logi dotyczące działań użytkowników.   
W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

3.6. Dostęp do logów historycznych.

System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

3.7. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log “customowy”). Ponadto CSB musi informować użytkownika/administratora o “nowych” zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a “nowe” logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

3.8. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).

System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

MODUŁ EDR/XDR

4.1. Integracja z systemem EDR/XDR. Wykonawca w ramach zamówienia dostarczy licencję (wraz z kluczami licencyjnymi umożliwiającymi instalację na 60 komputerach w Urzędzie) obowiązującą do 14.06.2026r. (Zamawiający dopuszcza podniesienie dotychczasowej wersji oprogramowania AV w celu osiągnięcia minimalnych wymagań opisanych poniżej)

* Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
* Rozwiązanie musi wspierać architekturę ARM64.
* Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
* Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
* Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
* Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
* Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
* Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
* Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
* Rozwiązanie musi integrować się z Intel Threat Detection Technology.
* Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta
* pocztowego).
* Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
* Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
* Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
* Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
* Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

* Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
* Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
* Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
* Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
* Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
* Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
* Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

* Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
* Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
* Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
* Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
* Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

* Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
* Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
* Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
* Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
* Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obumetod jednocześnie.
* Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
* Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
* Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

4.2. Podgląd informacji, alertów i zdarzeń występujących w środowisku IT

W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

4.3. Bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego)

Poza integracją i prezentacją incydentów/zdarzeń występujących na poszczególnych hostach   
w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.

MODUŁ INWENTARYZACJI

5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez “ręczne” wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany)   
z pozostałymi modułami systemu CSB.

5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja)

Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno   
w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu “ręcznym” system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

6.3.  Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

1. MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)

7.1. Integracja z systemem tiketowym.

System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

7.2.  Zgłaszanie incydentu/problemu, który został namierzony przez system.

Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów,   
a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku “Zgłoś Problem”. Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

7.3.  Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

1. MODUŁ WYKRYWANIA ZAGROŻEŃ

8.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.

System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających,   
czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

8.2.  Kategoryzacja oraz prezentacja wykrytych zagrożeń

System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte   
w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.

8.3.  Historia wykrytych zagrożeń

System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów  
 i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).

8.4.  Wsparcie/automatyczna ochrona po wykryciu zagrożenia

System musi posiadać możliwość włączenia “automatycznej ochrony” w wybrane dni tygodnia   
i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykona w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta na którym występuje zagrożenie.

MODUŁ RAPORTÓW

9.1.  Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów

System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administrator musie mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

PANEL UŻYTKOWNIKA

10.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością̨ serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

10.2. Wizualizacja statystyk zdarzeń i logów

Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości “nowych” zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

10.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo”.

Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na “żywo”, a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

10.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

10.5. Intuicyjny panel zarządzania regułami i definiowania “customowych” logów.

Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania “customowymi” logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych “customlogów” wraz   
z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu “customlogów” musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.

**Oprogramowanie do wykonywania kopii zapasowej**

Minimalne wymagane funkcje oprogramowania do backupu:

* kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal,
* kopia zapasowa środowisk MacOS
* kopia zapasowa maszyn wirtualnych (VMware, Hyper-V)
* kopia zapasowa serwerów fizycznych (Windows, Linux)
* obsługa wielu wersji i retencji,
* możliwość wyzwalania kopii zapasowej według harmonogramu,
* automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej,
* centralne zarządzanie,
* Oprogramowanie musi umożliwić tworzenie kopii zapasowej dla:
  + 55 komputerów stacjonarnych
  + 3 maszyn wirtualnych – uruchomionych dotychczas przez zamawiającego
  + Wszystkich maszyn wirtualnych dostarczonych/uruchomionych w ramach zamówienia.

**Certyfikowane, stacjonarne szkolenie z obsługi systemu do Back-up danych**

Wykonawca zapewni certyfikowane szkolenie (dla administratora z rozwiązania do tworzenia kopii zapasowych i ich odzyskiwania na urządzeniu zaproponowanym w ramach oferty -NAS) poprzez dostawę Zamawiającemu Vouchera . Szkolenie powinno zostać przeprowadzone na dostarczonym sprzęcie i przeprowadzone przez trenera, posiadającego odpowiednie kwalifikację z dostarczanego w ramach niniejszego zamówienia urządzenia NAS.

Sposób organizacji szkolenia

* Tryb wykonania: stacjonarne
* Czas trwania: 4 godziny

musi zawierać min. poniższe zagadnienia:

* Omówienie sposobu zarządzania kopiami
* Tworzenie planów kopii zapasowej
* Weryfikacja kopii zapasowej
* Odzyskiwanie kopii zapasowej

Administrator po szkoleniu powinien posiadać umiejętności dotyczące znajomość możliwości konfiguracji rozwiązania Systemu do Backupu i umiejętność samodzielnego wdrożenia rozwiązania na dostarczonym urządzeniu typu NAS

**Bezpieczne logowanie**

Mechanizm ma za zadanie znacznie poprawić bezpieczeństwo systemów poprzez zwiększenie kontroli nad dostępem, minimalizacją zagrożeń związanych z zarządzaniem hasłami i redukcję ryzyka ataków na konta użytkowników. Zapewnia centralne zarządzanie kontami użytkowników i dostępem do zasobów.

Wymagania niefunkcjonalne:

* Dostępność i wydajność: Zapewnienie szybkiego i niezawodnego mechanizmu logowania, aby użytkownicy mogli rozpocząć pracę z systemem bez opóźnień i problemów technicznych.
* Bezpieczne przechowywanie danych uwierzytelniających: Hasła i dane autoryzacyjne powinny być przechowywane w sposób bezpieczny z wykorzystaniem silnych algorytmów kryptograficznych, aby uniemożliwić odzyskanie oryginalnego hasła w przypadku naruszenia dostępu do systemu.
* Odporność na ataki: Mechanizm logowania powinien ograniczać liczbę prób nieudanych logowań aby uniemożliwić lub utrudnić atakującemu próby odgadnięcia hasła metodą brute force (np. blokada po 3 nieudanych próbach na 5 minut)
* Wymuszanie bezpieczeństwa: Mechanizm powinien umożliwić definiowanie własnej polityki bezpieczeństwa, tj wymagania co do długości hasła, złożoności (np. wymóg zawierania wielkich liter, małych liter, cyfr i znaków specjalnych) oraz okresowej zmiany hasła.
* Szyfrowanie danych: Wszystkie dane przesyłane w procesie logowania powinny być szyfrowane w celu ochrony przez przechwyceniem przez osoby trzecie.
* Bezpieczne zarządzanie sesjami: Mechanizm powinien umożliwić ograniczenie czasu trwania sesji oraz usuwać ją całkowicie po wylogowaniu użytkownika
* Monitorowanie aktywności: Mechanizm powinien rejestrować i monitorować aktywność logowania, w tym udane i nieudane próby logowania, aby wykrywać potencjalne próby naruszenia bezpieczeństw.
* Współpraca: Mechanizm bezpiecznego logowania powinien mieć możliwość konfiguracji i uruchomienia z kontrolerem domeny na środowisku z systemem Windows Serwer (np. Windows Serwer 2022) oraz Linux (Debian >= 12). Stacja końcowa (kliencka) musi być wyposażona w system Windows wpierający integrację z domeną tj. Professional bądź Enterprise.

Zakres integracji z obecnym systemem dziedzinowym

* W wyniku integracji mechanizmu bezpiecznego logowania z systemem dziedzinowym Respons autoryzacja użytkownika powinna nastąpić po uprzedniej skutecznej autoryzacji użytkownika na stacji roboczej, bez konieczności ponownego logowania bezpośrednio w systemie dziedzinowym.
* Pojedyncze logowanie powinno wyeliminować konieczność posiadania wielu różnych kont przez użytkowników.
* Integracja powinna być parametryzowana i opcjonalna.

Lista czynności dot. wdrożenia mechanizmu

* Aktualizacja systemu dziedzinowego na potrzeby uruchomienia mechanizmu bezpiecznego logowania.
* Wsparcie przy konfiguracja i mapowaniu użytkowników systemu dziedzinowego Respons z użytkownikami domeny.
* Instruktaże oraz asystę stanowiskową dla administratora.
* Świadczenie pomocy technicznej dotyczącej mechanizmu bezpiecznego logowania.
* Świadczenie usług utrzymania i konserwacji dla dostarczonego mechanizmu.
* Dostarczenie nowych wersji dokumentacji użytkownika wraz z nowymi wersjami systemu dziedzinowego i mechanizmu bezpiecznego logowania.

W pozycji obowiązkiem Wykonawcy będzie dostosowanie usług katalogowych dla użytkowników. Wdrożenie usług katalogowych nie może trwać dłużej niż do 90 dni przeznaczonych na realizację projektu.

Wdrożenie i skonfigurowanie usług katalogowych musi zapewniać efektywne zarządzania dostępem do zasobów informatycznych u Zamawiającego. Obowiązkiem Wykonawcy będzie utworzenie struktury organizacyjnej, grup, kont użytkowników oraz polityk bezpieczeństwa.

**Certyfikowane szkolenie z zarządzania Active Directory**

Wykonawca zapewni certyfikowane szkolenie (stacjonarne) dla administratora IT Zamawiającego z zakresu zarządzania usługami katalogowymi – Active Directory. Wykonawca dostarczy Zamawiającemu Voucher – uprawniający do odbycia szkolenia, które powinno zostać przeprowadzone przez trenera, posiadającego odpowiednie kwalifikację. W ramach szkolenia poruszone zostaną m.in. takie zagadnienia jak: instalacja i konfiguracja kontrolerów domeny, instalacja, konfiguracja i zarządzanie systemem DNS w ramach AD.

Voucher szkoleniowy musi obejmować szkolenie z poniższych zagadnień:

* Podstawowe pojęcia i architektura AD
* Role FSMO i ich znaczenie
* Struktura domeny, lasu i jednostek organizacyjnych (OU)
* Instalacja kontrolera domeny
* Podstawowe operacje na użytkownikach, grupach i jednostkach organizacyjnych
* Tworzenie, modyfikowanie i usuwanie kont użytkowników
* Profile użytkowników i polityki logowania
* Delegowanie uprawnień
* Tworzenie i edycja obiektów GPO
* Egzekwowanie i filtrowanie zasad
* Rozwiązywanie problemów związanych z GPO
* Mechanizmy zabezpieczeń w Active Directory
* Implementacja polityk haseł i uwierzytelniania wieloskładnikowego
* Monitorowanie logów zabezpieczeń
* Mechanizmy replikacji AD
* Narzędzia do diagnostyki i monitorowania replikacji
* Rozwiązywanie typowych problemów z replikacją

**Switch zarządzalny**

Minimalne wymagania techniczne:

* Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Możliwość instalacji redundantnego zasilacza
* Tablica MAC min. 16K
* Bufor 16Mb
* Wydajność min. 130 Mp/s
* Przepustowość min. 170 Gb/s
* Port USB
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Wymaga się aby urządzenie było objęte 5 letnią gwarancją producenta realizowaną w systemie door-to-door.

**UPS - stanowiskowy**

* Moc pozorna: nie mniej niż 1200 VA
* Moc rzeczywista: nie mniej 600 W
* Technologia: Line-Interactive
* Gniazda wyjściowe z podtrzymaniem bateryjnym typu E (2P+Z): minimum 4szt
* Parametry wejściowe:

Napięcie znamionowe: 220-240 V; 50/60 Hz

Zakres napięcia wejściowego: 140-300 V; 45-65 Hz

* Parametry wyjściowe

Znamionowe napięcie wyjściowe 220/230/240 V

Regulacja napięcia w trybie bateryjnym +/-20%

* Zdolność zwarciowa w trybie bateryjnym: 16A
* Wytrzymywany czas przepływu prądu zwarciowego 50 ms
* Czas przełączania: nie dłuższy niż 10 ms dla przejścia z trybu normalnego do trybu bateryjnego
* Zaawansowany monitoring z wczesnym wykrywaniem awarii oraz powiadamianiem.
* Zimny start
* Stopień ochrony: IP20
* Układ sieci UPS można podłączyć do układów zasilania TN, TT, IT, ten sam system jest dostarczany do obciążenia.
* Klasa ochronności Klasa I
* Temperatura pracy 0°C do 40°C (32°F do 104°F)
* Poziom hałasu <25 dBA
* Gwarancja 24 miesiące
* Gabaryty:

Wysokość: do 220 mm

Głębokość: do 380 mm

Szerokość: do 200 mm

* Waga: do 10kg

**UTM**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 10 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP 1 Gbps.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

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

# Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

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

# Funkcje SD-WAN

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

# Zarządzanie pasmem

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

# Ochrona przed malware

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

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

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

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

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

# Logowanie

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

# Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

b)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

# Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement).

**Certyfikowane szkolenie z urządzeń klasy UTM**

Wykonawca zapewni certyfikowany instruktaż (stacjonarny) dla administratora IT Zamawiającego z proponowanych urządzeń klasy UTM.

Instruktaż musi zawierać min. poniższe zagadnienia:

* Konfiguracja rozwiązania i jego implementacja
* Zbieranie logów i monitorowanie;
* konfiguracji sieci VPN IPSec VPN i SSL VPN
* Translacja adresów sieciowych (NAT);
* Translacja połączeń wychodzących/przychodzących oraz translacja dwukierunkowa
* Filtrowanie ruchu sieciowego (Firewall);
* Omówienie działania modułu IPS w tym różnice pomiędzy IPS a IDS
* Infrastruktura klucza publicznego
* SSL Proxy -zasada działania

**Serwer na potrzeby Centralnego Systemu Bezpieczeństwa**

**Minimalne wymagania**

|  |  |
| --- | --- |
| Parametr | Charakterystyka (wymagania minimalne) |
| Obudowa | Obudowa Rack o wysokości do 2U  Co najmniej 10 wnęk na dyski 3.5”  Obudowa wyposażona w panel LCD na froncie obudowy, pozwalający stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera.  Serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera zdalnie – np. przy użyciu dedykowanej aplikacji mobilnej |
| Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów.  Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci.  Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| Chipset | Dedykowany do pracy w serwerach dwuprocesorowych |
| Procesor | Zainstalowany procesor Intel Xeon Gold 5416S lub inny klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 282 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji jedno lub dwuprocesorowej lub osiągający w teście wydajności Passmark CPU Benchmark wynik 34 000 pkt. (w formularzu ofertowym należy wskazać oferowany model procesora) |
| RAM | Minimum 256GB |
| Kontroler RAID | Sprzętowy kontroler dyskowy, posiadając min. 8GB nieulotnej pamięci cache, możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  Wsparcie dla dysków samoszyfrujących |
| Dyski twarde | Zainstalowane:  3x dysk SSD o pojemności min. 480GB, Hot-Plug  4x dysk SAS o pojemności min. 2.4TB, Hot-Plug  Możliwość zainstalowania dysków M.2 NVMe SSD |
| Gniazda PCI | Cztery sloty PCIe umożliwiające rozbudowę macierzy |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |
| Wbudowane porty | 4 porty USB w tym min 1 port USB 3.0 z tyłu obudowy i 1 port micro USB z przodu obudowy  2 port VGA z czego jeden z przodu obudwy |
| Video | Zintegrowana karta graficzna |
| Wentylatory | Redundantne, Hot-Plug |
| Zasilacze | Redundantne, Hot-Plug min. 700W klasy Titanium |
| Elementy montażowe | Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych  Ramię / organizer do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| Bezpieczeństwo | Zatrzask górnej pokrywy, blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  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 |
| Karta Zarządzania – **w formularzu oferty należy podać pełną nazwę oferowanej karty** | Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej:  zdalny dostęp do graficznego interfejsu Web karty zarządzającej  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 SNMP; IPMI2.0, VLAN tagging, SSH  możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,  Wsparcie dla automatycznej rejestracji DNS  wsparcie dla LLDP  wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej  możliwość podłączenia lokalnego poprzez złącze RS-232.  możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.  Monitorowanie zużycia dysków SSD  możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,  Automatyczne zgłaszanie alertów do centrum serwisowego producenta  Automatyczne update firmware dla wszystkich komponentów serwera  Możliwość przywrócenia poprzednich wersji firmware  Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON  Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych  Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.  Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. |
| Oprogramowanie do zarządzania – **w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania** | Serwer musi umożliwiać zainstalowanie 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  Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| Wsparcie techniczne i oprogramowanie – **w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania** | Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego,  automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.  Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.  Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. |
| Warunki gwarancji | Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na **okres podany w ofercie**.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.  Zamawiający wymaga pojedynczego punktu kontaktu Producenta, w tym także dołączonego oprogramowania.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.  Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. |

**5. System operacyjny:**

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

* + Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
  + Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
  + Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych.
  + Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
  + Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
  + Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
  + Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
  + Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
  + Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a)  pozwalają na zmianę rozmiaru w czasie pracy systemu,

b)  umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c)  umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d)   umożliwiają zdefiniowanie list kontroli dostępu (ACL).

* Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
* Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
* Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
* Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
* Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
* Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a)  Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b)  Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

* Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
* Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
* Mechanizmy logowania w oparciu o:

a)   Login i hasło,

b)   Karty z certyfikatami (smartcard),

c)   Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

* Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
  + Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
  + Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
  + Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
  + Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji   
    w dokumentach (Digital Rights Management).
  + Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
  + Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a)  Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b)  Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.

d)  Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e)  Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

* Dystrybucję certyfikatów poprzez http
  + Konsolidację CA dla wielu lasów domeny,
  + Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
  + Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f)  Szyfrowanie plików i folderów.

g)  Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h)  Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i) Serwis udostępniania stron WWW.

j) Wsparcie dla protokołu IP w wersji 6 (IPv6),

k) Wsparcie dla algorytmów Suite B (RFC 4869),

l)  Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m)       Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
* Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
* Obsługi 4-KB sektorów dysków
* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
* Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
* Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
* Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
* Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
* Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
* Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
* Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Gwarancja

* 2 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej (**długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym**);
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

**Licencje dostępowe CAL**

W ramach zamówienia Wykonawca dostarczy 60 szt. licencji dostępowych do zaoferowanego serwerowego systemu operacyjnego.

**NAS - Network Attached Storage**

* + Obudowa RACK 19" 1U – wraz z kompletem szyn przesuwnych umożliwiających zamontowanie w szafie RACK
  + Procesor - liczba rdzeni nie mniej niż 4
  + Pamięć RAM - Minimum 8 GB, możliwość rozszerzenia pamięci RAM do 64GB
  + Liczba zatok na dyski twarde - Minimum 4
  + Obsługiwane dyski twarde:
  1. 3.5" SATA HDD / 2.5" SATA SSD – Hot Plug
  2. Zamawiający wymaga dostarczenia 4 dysków 3.5” SATA HDD o pojemności 8TB każdy o parametrach nie gorszych niż:

- Gwarancja – Zgodna z gwarancją zaproponowaną na urządzenie NAS.

- Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera.

- Dyski zgodne z listą kompatybilności producenta oferowanego serwera.

* Wbudowane kieszenie dysków M.2 NVMe - Minimum 2
* Możliwość podłączenia modułu rozszerzającego – Tak
* Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż: 16
* Porty na karty rozszerzeń - Minimum 1 x Gen3 x8 PCIe (x8 link)
* Porty LAN - Wbudowane min. 4 x 1GbE RJ-45
* Porty USB 3.2 - Minimum 2
* Gniazdo rozszerzenia - Minimum 1
* Zasilanie - Redundantny zasilacz o mocy minimalnej 150W
* Mechanizm szyfrowania sprzętowego - Tak, min AES-NI
* Wewnętrzny system plików BTRFS, EXT4
* Obsługiwane tryby RAID - JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny
* Uprawnienia - Uprawnienia listy kontroli dostępu systemu Windows (ACL)
* Usługa katalogowa - Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station
* Bezpieczeństwo - Zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
* Oprogramowanie
  + Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych
  + Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników.
  + Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego.
  + Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync
  + Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system
  + Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 60 jednoczesnych połączeń
* Gwarancja producenta serwera min 24 miesiące – **(długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym).**

**8. UPS**

* Moc pozorna - 3000 VA
* Moc rzeczywista - 3000 W
* Topologia (klasyfikacja IEC 62040-3) - Line-interactive z AVR
* Współczynnik mocy – 1
* Czas przełączenia na baterię - <4 ms
* Liczba, typ gniazd wyjściowych - 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
* Typ gniazda wejściowego - IEC C20 16A
* Czas podtrzymania dla 2500W obciążenia - 4 min
* Czas podtrzymania przy 1200W obciążenia -13 min
* Czas podtrzymania przy 3000W obciążenia -17 min
  + Dopuszcza się osiągnięcie czasu podtrzymania opisanego w punktach 8), 9), 10), za pomocą dodatkowych modułów bateryjnych.
* Dodatkowe baterie - Możliwość dodania do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 84 minut dla 2500W obciążenia przy pf=1,0
* Napięcie znamionowe - 200/208/220/230/240/250 V
* Tolerancja napięci prostownika - 160 V – 294 V (regulacja programowa 150-294 V)
* Częstotliwość znamionowa - 50/60 Hz autodetekcja
* Tolerancja częstotliwości - 47– 70 Hz
* Kształt napięcia – Sinusoidalny
* Napięcie znamionowe wyjściowe - 200/208/220/230/240 V do wyboru przez użytkownika
* Zakres zmian napięcia - +6/-10% napięcia nominalnego
* Częstotliwość wyjściowa - 50/60 Hz
* Współczynnik szczytu - 3:1
* Baterie wymieniane przez użytkownika "na gorąco" – Tak
* Ochrona przed przeładowaniem - Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
* Ochrona przed głębokim rozładowaniem - Tak
* Okresowy automatyczny test baterii – Tak
* Możliwość uruchomienia bez napięcia w sieci "zimny start" – Tak
* Baterie wewnętrzne o pojemności nie mniejszej niż - 9Ah 12V, minimum 6 szt.
* Czas ładowania baterii do poziomu 90% - < 3 godz. do 90% pojemności użytkowej
* Interfejs komunikacyjny:

1. USB
2. RS232 DB-9 żeński (HID)
3. styki przekaźnikowe
4. miniport wyłącznik ON/OFF
5. SNMP/Ethernet

* Panel sterowania z wyświetlaczem LCD:

1. Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
2. Poziomy rząd przycisków sterowania
3. Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
4. Sygnalizator akustyczny

* Sygnały akustyczne, co najmniej na awarię, niski stan naładowania baterii, przeciążenie, oraz konieczność serwisu.
* Przyciski sterujące i wskaźniki diodowe LED, co najmniej Przycisk Escape (anulowanie), Przyciski funkcyjne (przewijanie w górę i w dół), Przycisk Enter (potwierdzający), Przycisk ON/OFF załączenia i wyłączenia, LED trybu zasilania z siec i(kolor zielony), LED trybu baterii (kolor żółty), LED usterki (kolor czerwony).
* Typ obudowy uniwersalna Tower/Rack 2U
* Dane techniczne karty SNMP:

1. Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
2. Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
3. Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
4. Kamptybilność: SNMP v1/v3 i IP v4/v6
5. Interfejs: HTML5
6. Adresowanie IP: DHCP/BootP/Manualne
7. Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
8. Dostępny port USB (microUSB - port serwisowy)

* Dołączone oprogramowanie - Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów operacyjnych.
* Poziom hałasu w odl. 1m - do 40 dBA dla pracy normalnej
* Możliwość montażu ręcznego bypassu serwisowego
* Gwarancja producenta - 36 miesięcy dla elektroniki, 24 miesiące dla baterii (3 lata pełnej gwarancji po rejestracji produktu)