Załącznik nr 3 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Centralny System Bezpieczeństwa (SIEM z XDR, EDR, monitoringiem i zarządzaniem siecią) – 1 szt.

Przedmiot zamówienia obejmuje dostawę centralnego systemu bezpieczeństwa IT. Modernizacja musi obejmować wdrożenie poniższych funkcjonalności oraz spełniać co najmniej następujące minimalne wymagania techniczne i licencyjne:

W ramach postępowania Wykonawca jest zobowiązany zmodernizować/dostarczyć oprogramowanie wraz z licencją bezterminową dla 50 urządzeń. Oprogramowanie musi posiadać wsparcie do dnia 31.12.2026 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.

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 posiadać skalowalną architekturę dostosowaną do ilości urządzeń obsługiwanych w infrastrukturze Zamawiającego.

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 interfejs, 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.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

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 muszą spełniać standardy WCAG 2.1 na poziomie AA. Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami. Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie. Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie. Zgodność ze standardami HTML i CSS całego serwisu www. Kontrast kolorystyczny między tłem, a tekstem musi być 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:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.1. Moduł analizy podatności

1.1.1. 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.

1.1.2. 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.

1.1.3. 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).

1.2. Moduł monitoringu zasobów

1.2.1. 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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

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).

1. 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.

1. 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.

1.2.4. 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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

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.

1.2.5. 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).

1.2.6. 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.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.2.7. 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.

1.2.8. 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.

1.2.9. 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.

1.2.10. 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.

1.2.11. 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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

1.3. Moduł analizy logów

1.3.1. 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.

1.3.2. 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.

1.3.3. 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.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.3.4. 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.

1.3.5. 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.

1.3.6. 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.

1.3.7. 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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

1.4. Moduł EDR/XDR

System musi posiadać moduł EDR/XDR, stanowiący zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń.

Moduł musi posiadać 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.

Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender). System musi umożliwiać bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje takie jak automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.

1.5. Moduł inwentaryzacji

1.5.1. 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.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.5.2. 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.

1.5.3. 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.

1.6. Moduł zgłaszania incydentów (e-mail, system help-deskowy)

1.6.1. 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.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.6.2. 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.

1.6.3. 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.

1.7. Moduł wykrywania zagrożeń

1.7.1. 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.

1.7.2. 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.

1.7.3. Historia wykrytych zagrożeń

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

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).

1.7.4. 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.

1.8. Moduł raportów

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.

1.9. Panel użytkownika

1.9.1 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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

1.9.2. 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.

1.9.3. 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).

1.9.4. 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.

1.9.5. 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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

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.

1.10. Moduł analizy danych AI

System musi posiadać moduł analizy AI (sztucznej inteligencji) ułatwiający analizę danych agregowanych w systemie. Sztuczna inteligencja w postaci wirtualnego asystenta musi analizować szereg danych pochodzących z pozostałych modułów systemu, co najmniej modułu monitoringu zasobów, modułu logów oraz modułu wykrywania zagrożeń. Wirtualny asystent musi analizować dane pod kątem cyberbezpieczeństwa z naciskiem na określenie poziomu ryzyka oraz sposobu zabezpieczenia.

1.10.1. Analiza bieżących logów

Moduł musi umożliwiać użytkownikowi uruchomienie asystenta AI do przeanalizowania logów po kątem cyberbezpieczeństwa. Asystent po uruchomieniu musi przeanalizować bieżące logi uwzględniając w analizie co najmniej logi skategoryzowane w systemie jako błędy. Asystent AI musi przeanalizować logi pochodzące z każdego hosta/urządzenia dodanego w module inwentaryzacji. Ponadto Asystent AI musi szacować ryzyko zagrożenia określając jego poziom (Ryzko: wysokie, średnie, niskie) podawać wynik analiz w postaci opisu przeanalizowanych błędów (na co wskazują i czego dotyczą) oraz sugerować reguły, które należy włączyć, aby zmniejszyć ryzyko cyberataku. Asystent AI musi pytać użytkownika, czy włączyć automatycznie zabezpieczenia (reguły), których włączenie zaleca po analizie logów. Wynik analizy powinien również sugerować i krótko opisać techniki (z matrycy Mitre ATT&CK) cyberataków, których mogą dotyczyć.

1.10.2. Analiza wykrytych zagrożeń

Moduł musi umożliwić użytkownikowi uruchomienie asystenta AI w celu dokonania analizy raportowanych wpisów w module wykrywania zagrożeń. Asystent do analizy powinien brać wszystkie zagrożenia wykryte obecnego dnia z poszczególnych hostów dodanych w module inwentaryzacji. Wynikiem analizy musi być podsumowanie (opis) najważniejszych informacji zawierający w szczególności dane na temat możliwości wystąpienia cyberataku. Asystent musi sugerować, co należy zrobić, aby przeciwdziałać wykrytym zagrożeniom.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.10.3. Analiza problemów

Moduł musi umożliwić użytkownikowi uruchomienie asystenta AI w celu przeanalizowania problemów występujących na poszczególnych hostach zaraportowanych w module monitoringu zasobów. Asystent musi dokonać analizy wszystkich problemów niezależnie od ich priorytetów zgłoszonych w danym dniu. W wyniku analizy asystent AI musi sugerować działania ułatwiające użytkownikowi rozwiązanie zgłoszonych w systemie problemów. Sugestie te powinny zawierać informację na temat możliwych przyczyn występowania tych problemów oraz opisać zalecane czynności umożliwiające ich rozwiązanie.

1.11. Moduł threat intelligence

System musi mieć moduł umożliwiający analizę danych dotyczących potencjalnych zagrożeń oraz wskaźników kompromitacji (IoC) zidentyfikowanych przez źródła zewnętrzne takie jak AbuseCH. Moduł musi uwzględniać różne kategorie danych (wskaźników kompromitacji) dotyczących co najmniej informacji o złośliwym oprogramowaniu (malware), zagrożeniach sieciowych oraz zgłoszonych złośliwych adresach URL.

1.11.1. Lista wskaźników – MALWARE

Lista wskaźników dotyczących złośliwego oprogramowania musi zawierać istotne informację na temat zgłoszonego zdarzenia. Na liście tej muszą się znaleźć co najmniej informację na temat: czasu zdarzenia, wskaźnika wykrycia, rozmiaru pliku, typu pliku, kategorii zdarzenia, nazwy źródła, daty pierwszego wykrycia, Hash MD5, Hash ssdeep, Hash TLSH. Ponadto użytkownik systemu musi mieć możliwość dodania wybranego zawirusowanego pliku do listy blokowanych plików oraz jeśli dany wskaźnik kompromitacji został określony i opublikowany np. na witrynie virustotal.com, to użytkownik musi mieć możliwość automatycznego przekierowania do źródła z odfiltrowaniem danych do wybranego zdarzenia.

1.11.2. Lista wskaźników – zagrożenia sieciowe

Lista wskaźników dotyczących zagrożeń sieciowych musi zawierać istotne informację na temat zgłoszonego zdarzenia. Lisa ta musi zawierać co najmniej informację na temat: czasu zdarzenia, nazwy złośliwego oprogramowania, opisu zagrożenia, poziomu zaufania, adresu (portu) bądź Hashu pliku, typu wskaźnika, kategorii zdarzenia, czasu pierwszego wykrycia, nazwy źródła oraz dostawcy wskaźnika. Ponadto podobnie jak w przypadku wskaźników malware użytkownik powinien mieć dostęp z poziomy modułu do źródła zawierającego więcej szczegółowych informacji.

1.11.3. Lista wskaźników – złośliwe adresy URL

Lista wskaźników dotyczących złośliwych adresów URL musi zawierać istotne informację na temat zgłoszonych zdarzeń. Lista ta musi zawierać informację dotyczące co najmniej: czasu zdarzenia, adresu URL,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

statusu adresu, rodzaju zagrożenia, typu wskaźnika, kategorii zdarzenia, nazwy źródła, czasu pierwszego wystąpienia, dostawcy wskaźnika, listy Spamhaus DBL oraz listy SURBL. Ponadto podobnie jak w przypadku poprzednich wskaźników użytkownik powinien mieć dostęp z poziomy modułu do źródła zawierającego więcej szczegółowych informacji.

1.11.4. Lista blokowanych plików

Moduł powinien umożliwiać użytkownikowi wyświetlenie listy plików przez niego zablokowanych na liście wskaźników typu malware. Umieszczone na tej liście pliki muszą być wykrywane przez agentów systemu i blokowane w celu ochronienia poszczególnych hostów. Użytkownik powinien mieć również możliwość ręcznego dodawania plików do tej listy poprzez podanie farmatu hash pliku, nazwy, krótkiego opisu, hashu pliku oraz systemu operacyjnego. Użytkownik musi mieć możliwość dodawania do blokady plików dla co najmniej trzech głównych systemów operacyjnych tj. windows, linux, MAC IOS.

1.11.5. Wyszukiwanie i filtrowanie

Moduł dotyczący wskaźników kompromitacji musi być wyposażony w intuicyjną wyszukiwarkę umożliwiającą zaawansowane wyszukiwanie po treści informacji oraz filtrującej po kategoriach danych oraz wybranym zakresie dat.

1.12. Moduł UEBA

System musi być wyposażony w moduł UEBA umożliwiający wykrywanie anomalii i podejrzanych zachowań użytkowników. System przy wykorzystaniu modeli ML (Machine Learning) musi automatycznie wykrywać podejrzane aktywności użytkowników UBA oraz nietypową pracę infrastruktury EBA.

1.12.1. Predefiniowane reguły wykrywania anomalii UEBA

System musi być wyposażony predefiniowane reguły wykrywania anomalii przy wykorzystaniu modeli ML dotyczących zarówno analizy behawioralnej użytkowników UBA jak i działania infrastruktury EBA. System musi być wyposażony co najmniej w reguły dotyczące:

- podejrzanej aktywności systemów, reguła musi analizować zdarzenia systemowe, takie jak zmiany w rejestrze, zmiany czasu systemowego, zmiany w konfiguracji rozruchu czy instalacje aktualizacji, w celu wykrycia nietypowych działań mogących sugerować próbę manipulacji lub nieautoryzowanego dostępu do systemu,
- zapytań DNS do podejrzanych lokalizacji geograficznych, reguła musi analizować zapytania do serwerów DNS znajdujących się w nietypowych krajach w stosunku do standardowego ruchu organizacji, mogących wskazywać na działania związane z malwarem lub wyciekiem danych,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- potencjalnego zachowania użytkowników wskazujące na atak typu DDoS, reguła musi umożliwiać detekcje nietypowej intensywności aktywności użytkownika, mogącej sugerować atak rozproszonego typu (DDoS) lub infekcję systemu,
- nietypowych zachowań użytkowników w zdarzeniach bezpieczeństwa, reguła musi analizować nietypowe wzorce aktywności użytkowników, takie jak nagły wzrost liczby zdarzeń bezpieczeństwa lub działania poza standardowymi godzinami pracy,
- podejrzanych logowań lub eskalacji uprawnień, reguła musi wykrywać anomalie, w zachowaniach takich jak logowania z nieznanych lokalizacji lub kont o wysokich uprawnieniach.

1.12.2. Parametryzacja i trenowanie zaimplementowanych modeli ML

System musi dawać możliwość trenowania zaimplementowanych modeli ML oraz ich automatyczne douczanie. W systemie musi być możliwość wybrania detektora dla wybranej reguły UEBA i podglądnięcia jego parametrów. W systemie musi być możliwość sprawdzenia algorytmów użytych do analizy wraz z dopasowanymi parametrami i oceną ryzyka. Ponadto w ustawieniach detektorów muszą znaleźć się takie informację jak status modelu, data ostatniego treningu, oraz metryki cech modelu użyte do analizy wraz ze statystykami (min, max, średnia, najczęstsza wartość itp.). Ponadto użytkownik systemu musi mieć możliwość zmiany parametrów detektora użytego w wybranej regule i przetrenowania modelu na nowo. W przypadku detektorów uczących się na bieżąco zmiany parametrów i uruchomienia detektora na nowo. Trenowanie detektorów musi odbywać się w tle i nie zaburzać działania systemu w zakresie pozostałych detektorów oraz funkcjonalności.

1.12.3. Prezentacja i wizualizacja wykrytych anomalii

System musi umożliwiać użytkownikom prześledzenie rozkładu zdarzeń i anomalii w czasie zaprezentowanych na intuicyjnym wykresie. Ponadto w systemie musi być możliwość sprawdzenia wystąpienia anomalii w formie tabelarycznej. Lista anomalii musi zawierać dane używane w detektorach takie jak np. czas wystąpienia zdarzenia, czy nazwa hosta, którego dotyczy zdarzenie. Ponadto system musi posiadać funkcjonalność umożliwiającą wybranie zgłoszonej anomalii i zatwierdzenia jej jako anomalii dopuszczonej przez administratora systemu. Zatwierdzone przez administratora anomalie stanowić mają wykluczenie dla detektorów w kolejnych analizach danych.

1.12.4. Wektor ataku

System musi być wyposażony w funkcjonalność umożliwiającą wybranie zgłoszonej anomalii i sprawdzenie jak potencjalne zagrożenie przebiegało w infrastrukturze IT. Wektor ataku powinien być

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

przedstawiony w postaci interaktywnej mapy sieci, przedstawiającej te elementy infrastruktury, przez które przeszedł potencjalny cyberatak.

1.12.5. Wyszukiwanie i filtrowanie

Moduł musi być wyposażony w intuicyjną wyszukiwarkę umożliwiającą zaawansowane wyszukiwanie po danych biorących udział w analizie (cechy detektorów) oraz filtrującej po kategoriach danych oraz wybranym zakresie dat.

1.13. Moduł obsługi zgłoszeń

1.13.1. Moduł obsługi zgłoszeń pozwalający na przeglądanie i obsługę zgłoszeń pochodzących od użytkowników z różnych jednostek organizacyjnych

Moduł musi umożliwiać pełną kontrolę nad cyklem życia zgłoszenia – od rejestracji, przez klasyfikację, aż po finalne rozwiązanie. Moduł musi posiadać adres URL do formularza zgłoszeń umożliwiający użytkownikom z innych jednostek organizacyjnych zgłaszać incydenty lub podejrzane naruszania bezpieczeństwa. Formularz zgłoszeniowy musi zawierać następujące pola: imię i nazwisko, adres e-mail, temat, wiadomość. Wysyłanie zgłoszeń musi być zabezpieczone mechanizmem reCAPTCHA.

1.13.2. Filtr ułatwiający wyszukiwanie zgłoszeń po statusie: nowe, w obsłudze, odrzucone, obsłużone oraz zamknięte.

Każde nowe zgłoszenie musi być widoczne w liście zgłoszeń posiadać identyfikator, datę utworzenia, dane zgłaszającego, zgłoszenie oraz status. Administrator musi mieć możliwość zmian statusów zgłoszeń wraz z dodaniem komentarza opisującego wykonane podczas obsługi czynności, a w przypadku odrzucenia zgłoszenia podania przyczyny. Wszystkie zmiany statusów muszą być zapisywane chronologicznie i być dostępne przy każdym zgłoszeniu. Zgłoszenia nie mogą być usuwane z systemu przez użytkowników, każde zgłoszenie musi pozostać w historii modułu.

1.13.3. Oddzielna wyszukiwarka

Moduł obsługi zgłoszeń musi posiadać oddzielną wyszukiwarkę umożliwiającą użytkownikowi szybkie wyszukanie zgłoszenia.

1.14. Moduł symulacji ataku

System musi być wyposażony w moduł symulacji ataku umożliwiający sprawdzenie zabezpieczeń wprowadzonych w jednostce. System musi dawać możliwość uruchomienia agenta testującego na co najmniej trzech typach systemów operacyjnych (Windows, Linux, iOS). W module symulacji powinna znajdować się krótka instrukcja instalacji agentów na wybranym środowisku operacyjnym. Moduł musi być wyposażony w

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

wyszukiwarkę kontekstową przeszukująca po polach dostępnych dla listy agentów, Scenariuszy oraz utworzonych i wykonanych symulacji.

1.14.1. Scenariusze ataków

System musi być wyposażony w co najmniej 25 różnych scenariuszy umożliwiających testowanie zabezpieczeń. Scenariusze te powinny testować możliwości takie jak min: Screen Capture, Copy Clipbard, Get Chrome Bookmarks, Record microphone, Create staging direcotry, Find files, Stage sensitive files, Compress staged directory, Exfil staged direcotry, Discover Antivirus programs, Scan WIFI networks, Sniff network traficc, Add bookmark, Avoid logs, Disable Windows Defender All, Move Powershell & trage, Clear Logs, Advanced File Search and Stager, Compress staged directory, Exfil Compressed Archive to FTP Server, WMIC Process Enumeration, tsklist Process Enumeration, PowerShell Process Enumeration, UAC Status, SysInternals PSToll Process Discovery, Identify active user, Collect ARP details, Identify system processes, Prefered WIFI, Disript WIFI, Rverse nslookup IP, View remote shares, Copy 54ndc47 (SMB), Start 54ndc47 (WMI), Parse SSH config, Dump history, View admin shares, Run PowerKatz, Find Hostname, Reverse nslookupIP, Mount Share, Start Agent (WinRM), UAC bypass registry, wow64log DLL Hijack, duser/osksupport DLL Hijack, Bypass UAC Medium, Manx, Levarage Procdump for Isass memory, Signed Binary Execution – odbcconf, Signed Binary Execution – Mavinject oraz wiele innych. Wybór predefiniowanego scenariusza musi odbywać się z poziomu UI systemu.

1.14.2. Symulacje ataków

System musi umożliwiać tworzenie symulacji ataków wykonywanych na dodanych agentach wg. wybranego scenariusza. Podczas dodawania nowej symulacji użytkownik systemu/administrator musi mieć możliwość podania co najmniej: nazwy symulacji, wyboru scenariusza z listy oraz wybrania algorytmu szyfrującego w celu utrudnienia wykrycia podejrzanych zachowań. Użytkownik musi mieć do wyboru, co najmniej algorytm Base64, Base64jumble, Base64noPadding lub wybrać przebieg symulacji bez szyfrowania. Po wykonaniu symulacji w systemie musi znajdować się informacją na temat jej przebiegu na dodanych agentach. Po wyświetleniu szczegółów przebiegu symulacji w systemie muszą znajdować się informację takie jak: Data rozpoczęcia symulacji, nazwa wykonywanej operacji (np. Current USer) nazwa taktyki/techniki z MITRE (np. discovery TI033 – Sytem Owner/User Discovery), nazwa agenta, PID, Status (wykonano, niepowodzenie, brak odpowiedzi) oraz wykonywane polecenie po i przed zaszyfrowaniem. Oprócz polecenia w systemie powinna być również zapisana odpowiedź z testowanego środowiska (agenta).

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.15. Moduł SLA

System musi być wyposażony w moduł SLA umożliwiający monitorowanie i obsługę incydentów przez administratorów systemu. W Module SLA musi być możliwość obsługi incydentów zgłaszanych przez system w pozostałych modułach, a w szczególności z podatności z Modułu analizy podatności, Problemów z Modułu monitoringu zasobów, zagrożeń z Modułu wykrywania zagrożeń oraz incydentów zgłaszanych przez zintegrowany system EDR w module EDR. Moduł musi być wyposażony w wyszukiwarkę kontekstową umożliwiającą wyszukanie zdarzenia po dostępnych w listach zdarzeń polach. Ponadto system musi umożliwiać filtrowanie zdarzeń SLA po ich statusach.

1.15.1. Ustawienia SLA

System musi być wyposażony w panel konfiguracyjny umożliwiający włączenie/wyłączenie kontroli SLA, nadanie czasu reakcji oraz czasu obsługi zdarzenia (incydentu). Ustawienia te muszą być możliwe dla statusów zdarzeń osobno. W systemie musi być możliwość skategoryzowania zdarzeń poprzez nadawanie im statusów. Każdy incydent pojawiający się w module SLA automatycznie musi być przypisany do kategorii nowe zdarzenie. administratorzy/użytkownicy systemu muszą mieć możliwość zmiany tego statusu na np. segregacja, incydent bezpieczeństwa, fałszywy alarm oraz zdarzenie obsłużone. Ponadto system musi dawać możliwość przypisywania różnych parametrów SLA dla zdarzeń pochodzących z różnych powyżej wymienionych modułów systemu. W ustawieniach SLA użytkownik systemu musi mieć możliwość ustawienia limitów dotyczących ilości wierszy w powiadomieniach, osobno dla powiadomień mailowych i osobno dla powiadomień sms’owych. Moduł SLA musi być również wyposażony w kreator reguł powiadomień SLA umożliwiający administratorom/użytkownikom tworzenie własnych reguł powiadomień. W konfiguracji reguły musi by możliwość nadania nazwy własnej reguły, zdefiniowania odbiorców powiadomień min: Operator przypisany do typu zdarzenia, grupa odbiorców (np. użytkownicy należący do grupy Administratorzy), właściciela zasobu/usługi oraz zewnętrznego odbiorcy poprzez podanie adresu e-mail i/lub numeru telefonu, wybrania kanału powiadomienie email i/lub sms oraz dodanie warunku, po którego spełnieniu zostanie wysłane powiadomienie. Administrator/użytkownik systemu musi mieć możliwość tworzenia reguł wielowarunkowych, w których użytkownik wybiera operator logiczny OR lub AND określając przy tym czy wszystkie warunki muszą być spełnione, czy wystarczy tylko jeden z nich aby powiadomienia zostały wysłane. Lista warunków powiadomień musi zawierać min.: Przekroczono czas reakcji SLA, Przekroczono czas obsługi SLA, Przekroczono SLA reakcji o określony czas, Przekroczono czas obsługi o określony czas, Zbliżenie do przekroczenia SLA reakcji, Zbliżenie do przekroczenia SLA obsługi, Osiągnięty priorytet dla CVE, Osiągnięty priorytet dla zagrożenia, osiągnięty priorytet dla alertu (problemu), krytyczny zasób, Zdarzenie na zasobie danych osobowych.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1.15.2. Lista zdarzeń dla podatności CVE

Moduł SLA musi posiadać listę zdarzeń dotyczącą podatności CVE. Każde nowe zdarzenie CVE zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, Daty utworzenia, numeru CVE, informacji na temat urządzenie i oprogramowania którego dotyczy, czas reakcji i obsługi, status. W sytuacji gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów CVE, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń CVE musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

1.15.3. Lista zdarzeń dla problemów

Moduł SLA musi posiadać listę zdarzeń dotyczącą problemów zgłaszanych w module monitoringu zasobów. Każde nowe zdarzenie zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, Daty utworzenia, treści problemu, informacji na temat urządzenia i oprogramowania którego dotyczy, czas reakcji i obsługi, status. W sytuacji gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów problemu którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących problemów musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

1.15.4. Lista zdarzeń dla zagrożeń

Moduł SLA musi posiadać listę zdarzeń dotyczącą zagrożeń wykrytych w module wykrywania zagrożeń. Każde nowe zdarzenie zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, Daty utworzenia, powodu wystąpienia zdarzenia, informacji na temat urządzenia którego dotyczy, czas reakcji i obsługi, status. W sytuacji gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów zagrożenia, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących zagrożeń musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

1.15.5. Lista Incydentów EDR

Moduł SLA musi posiadać listę zdarzeń dotyczącą incydentów zgłoszonych w module EDR. Każde nowe zdarzenie zgłoszone przez system musi zawierać informację na temat: Identyfikatora, Przypisanego Operatora, daty utworzenia, zgłoszonej nazwy incydentu, informacji na temat urządzenia którego dotyczył, czas reakcji i obsługi, status. W sytuacji gdy czas reakcji lub obsługi został przekroczony system musi przedstawiać czas opóźnienia zaznaczając go kolorem czerwonym. W module administrator/użytkownik musi mieć możliwość wyświetlenia szczegółów incydentu, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących incydentów EDR musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

1.16. Moduł SOAR

Moduł SOAR musi stanowić rozszerzenie funkcjonalności systemu klasy SIEM i będzie odpowiadał za automatyzację oraz standaryzację reakcji na incydenty bezpieczeństwa raportowane w systemie SIEM. Moduł ten musi integrować ze sobą różne elementy systemu SIEM takie jak procesy detekcji MITRE, podatności CVE, reguły korelacyjne, czy anomalie UEBA z procesami działań reakcyjnych w jednym, spójnym środowisku. Podsumowując Moduł SOAR musi umożliwiać skrócenie czasu reakcji na incydenty bezpieczeństwa oraz automatyzację reakcji na ich wystąpienie bez konieczności ręcznej interwencji.

1.16.1. Automatyzacja reakcji na incydenty bezpieczeństwa

System musi automatycznie inicjować odpowiednie scenariusze reakcji (playbooki) po wykryciu zdarzenia spełniającego zdefiniowane warunki. Scenariusze muszą uwzględniać co najmniej: korelację zdarzeń z wielu źródeł, poziomu ryzyka (poziom istotności) i priorytetyzację incydentów bezpieczeństwa oraz obszarów zagrożeń i zdefiniowanych grup, automatyczne wykonywanie działań naprawczych (np. izolacja hosta, blokada adresu IP, dezaktywacja kont użytkowników), możliwość warunkowa eskalacji incydentów oraz sposobu alertowania.

1.16.2. Wizualizacja procesów bezpieczeństwa

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

System musi zapewniać graficzną wizualizację procesów reagowania (playbook) na wykryte incydenty bezpieczeństwa. System musi udostępniać intuicyjne mapy procesów , prezentujące:

- kolejne etapy obsługi incydentu,
- zależności pomiędzy poszczególnymi krokami,
- warunki logiczne,
- punkty automatyzacji oraz eskalacji i alertowania.

1.16.3. Zarządzanie playbookami

Moduł SOAR musi posiadać centralną listę playbooków, zawierającą co najmniej następujące informacje:

- nazwę playbooka,
- datę i godzinę utworzenia,
- liczbę kroków,
- status playbooka (włączony/ wyłączony).

System musi umożliwiać:

- włączanie i wyłączanie playbooków,
- edycję playbooków,
- trwałe usuwanie playbooków,
- podgląd szczegółowej struktury playbooka.

Lista playbooków musi posiadać funkcje sortowania oraz eksportu do plików CSV, PDF oraz HTML.

1.16.4. Tworzenie i edycja playbooków

Wymagane jest, aby tworzenie playbooków odbywało się w sposób standaryzowany , poprzez:

- wprowadzenie unikalnej nazwy playbooka,
- definiowanie kroków reakcji poprzez wybór wyzwalacza, skryptu, akcji z predefiniowanych list.

System musi umożliwiać budowę playbooków wieloetapowych, zawierających jeden , lub wiele warunków logicznych.

1.16.5. Wyzwalacze

Moduł SOAR musi zawierać listę predefiniowanych wyzwalaczy , obejmujących w szczególności:

- wysokie użycie CPU,
- cykliczne uruchomienie playbooka,
- przeciążenie dysku,
- zbyt wysokie opóźnienia odczytu lub zapisu dysku,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- wysokie wykorzystanie pamięci RAM,
- wykrycie nowego zagrożenia wg. MITRE ATT&CK
- wykrycie nowego zagrożenia na podstawie zdefiniowanych reguł korelacyjnych
- wykrycie nowej podatności CVE,
- wykrycie potencjalnie niebezpiecznej wiadomości e-mail (MS Exchange), - wykrycie anomalii behawioralnych (UEBA).

1.16.6. Skrypty

Moduł SOAR musi umożliwiać uruchamianie skryptów, w tym w szczególności:

- analizę zajętości katalogów,
- pobieranie listy procesów,
- izolację hosta z sieci,
- zrzut pamięci procesu,
- zatrzymanie procesu,
- anulowanie izolacji hosta.

1.16.7. Akcje

Moduł SOAR musi obsługiwać akcje lokalne oraz akcje wykonywane w systemach zewnętrznych, w szczególności:

- systemy pocztowe (MS Exchange),
- zapory sieciowe (FortiGate),
- systemy zarządzania infrastrukturą sieciową (HPE IMC).

System musi umożliwiać m.in.:

- zarządzanie wiadomościami e-mail i kwarantanną,
- blokowanie adresów IP na zaporach sieciowych,
- zmianę statusów interfejsów sieciowych,
- wysyłanie powiadomień,
- wykonywanie testów łączności (PING).

1.16.8. Incydenty SOAR

Moduł SOAR powinien zawierać dedykowany obszar zarządzania incydentami SOAR, obejmujący pełny cykl życia incydentu:

- wykrycie zdarzenia,
- korelację,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- uruchomienie playbooków,
- realizację etapów reakcji,
- zatwierdzenie działań (jeśli wymagane), - zamknięcie incydentu.

1.16.9. Lista incydentów SOAR

System musi udostępniać listę incydentów, która:

- umożliwia filtrowanie po dacie,
- umożliwia wyszukiwanie rekordów,
- umożliwia sortowanie wyników,
- umożliwia eksport do CSV, PDF oraz HTML. Każdy incydent musi zawierać:
- nazwę playbooka,
- nazwę hosta lub zasobu,
- opis incydentu,
- datę i godzinę utworzenia, - typ lub identyfikator incydentu, -liczbę zrealizowanych etapów.

1.16.10. Szczegóły incydentu

System powinien umożliwiać szczegółowy podgląd incydentu, w tym:

- listę etapów playbooka,
- nazwę etapu,
- typ etapu (wyzwalacz / skrypt / akcja),
- opis,
- datę i godzinę uruchomienia,
- status wykonania,
- dane kontekstowe właściwe dla danego typu akcji (np. odbiorcy wiadomości).

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2. Dostawa serwera rozwiązań cyberbezpieczeństwa – 1 szt.

Urządzenie ma spełniać następujące parametry techniczne, funkcjonalności oraz warunki udzielonej gwarancji producenta:

2.1. Obudowa

- Typu RACK, wysokość nie więcej niż 1U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;
- Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD SATA Hot-Plug 480 GB;
- Zainstalowane 4 szt. dysków SAS/NL-SAS Hot-Plug 2,4 TB.

2.2. Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 86-rdzeniowych;
- Moduł TPM 2.0;
- 32 gniazda pamięci RAM;
- Obsługa 8 TB pamięci operacyjnej RAM DDR4;
- Obsługa pamięci MRDIMM.**Procesory;**
- Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,3 GHz, architektura x86_64;
- osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 535 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/ dla oferowanego serwera.

2.3. Pamięć RAM

- 128 GB pamięci RAM;
- DDR5 Registered 6400MT/s.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2.4. Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: 4 x 1Gbit Base-T w tym 1 szt. do zarządzania OOB serwerem;

2.5. Kontrolery RAID

Kontroler SAS RAID obsługujący następujące poziomy RAID: 0,1,10, posiadający wsparcie dla dysków SED.

2.6. Porty

- Zintegrowana karta graficzna ze złączem Display Port;
- 4 porty USB 3.2;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

2.7. Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

2.8. Zarządzanie

2.8.1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii

Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

- karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
- procesory CPU;
- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
- status karty zarządzającej serwera;
- wentylatory;
- bateria podtrzymująca ustawienia BIOS płyty głównej;
- zasilacze.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2.8.2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web, SSH;
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
- Zarządzanie alarmami (zdarzenia poprzez SNMP);
- Możliwość przejęcia konsoli tekstowej;
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
- Obsługa serwerów proxy (autentykacja);
- Obsługa VLAN;
- Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
- Obsługa protokołów TLS 1.2,
- Obsługa protokołu LDAP;
- Synchronizacja czasu poprzez protokół NTP;
- Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej.

2.8.3. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);

2.8.4. Serwer z możliwością konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera

2.9. Wspierane/Certyfikowane OS

- Microsoft Windows Server 2025, 2022;
- VMWare vSphere 9.x,8.x;
- Suse Linux Enterprise Server 15, 16;
- Red Hat Enterprise Linux 9.x, 10.x,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Oracle Linux 9.x, 10.x,
- XenServer 8.4

2.10. Gwarancja

- 5 lat gwarancji producenta serwera w trybie on-site w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników;
- 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 (podać koszt na dzień składania oferty).

2.11. Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
- Zgodność z normami: RoHS, WEEE oraz CE.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

3. Serwer Centrum Zgłaszania Awarii – 1 szt.

Urządzenie ma spełniać następujące parametry techniczne, funkcjonalności oraz warunki udzielonej gwarancji producenta:

3.1. Obudowa

- Typu RACK, wysokość nie więcej niż 1U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;
- Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD SATA Hot-Plug 480 GB;
- Zainstalowane 4 szt. dysków SAS/NL-SAS Hot-Plug 2,4 TB.

3.2. Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 86-rdzeniowych;
- Moduł TPM 2.0;
- 32 gniazda pamięci RAM;
- Obsługa 8 TB pamięci operacyjnej RAM DDR4;
- Obsługa pamięci MRDIMM.

3.3. Procesory

- Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,3 GHz, architektura x86_64;
- osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 535 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/ dla oferowanego serwera.

3.4. Pamięć RAM

- 128 GB pamięci RAM;
- DDR5 Registered 6400MT/s.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

3.5. Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: 4 x 1Gbit Base-T w tym 1 szt. do zarządzania OOB serwerem.

3.6. Kontrolery RAID

Kontroler SAS RAID obsługujący następujące poziomy RAID: 0,1,10, posiadający wsparcie dla dysków SED.

3.7. Porty

- Zintegrowana karta graficzna ze złączem Display Port;
- 4 porty USB 3.2;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

3.8. Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

3.9. Zarządzanie

Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

- karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
- procesory CPU;
- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
- status karty zarządzającej serwera;
- wentylatory;
- bateria podtrzymująca ustawienia BIOS płyty głównej;
- zasilacze.

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web, SSH;
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
- Zarządzanie alarmami (zdarzenia poprzez SNMP);
- Możliwość przejęcia konsoli tekstowej;
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
- Obsługa serwerów proxy (autentykacja);
- Obsługa VLAN;
- Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
- Obsługa protokołów TLS 1.2,
- Obsługa protokołu LDAP;
- Synchronizacja czasu poprzez protokół NTP;
- Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej.

Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna).

Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera.

3.10. Wspierane/Certyfikowane OS

- Microsoft Windows Server 2025, 2022;
- VMWare vSphere 9.x,8.x;
- Suse Linux Enterprise Server 15, 16;
- Red Hat Enterprise Linux 9.x, 10.x;
- Oracle Linux 9.x, 10.x;
- XenServer 8.4.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

3.11. Gwarancja

- 5 lat gwarancji producenta serwera w trybie on-site w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników;
- 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 (podać koszt na dzień składania oferty).

3.12. Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
- Zgodność z normami: RoHS, WEEE oraz CE.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4. System operacyjny do serwera – 1 szt.

4.1. Warunki licencji

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 dla serwerów opisanych w punkcie 2 i 3. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

4.2. Cechy systemu operacyjnego

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);

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- 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;
- 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,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

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,

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,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- 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.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

5. Usługa wirtualizacji – 1 usługa

Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie (w ramach dostarczonego systemu operacyjnego):

- Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta;
- Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta;
- Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach;
- Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów;
- Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy;
- Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN;
- Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q;
- Przygotowanie koncepcji wirtualizacji fizycznych maszyn;
- Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym;
- Konfiguracja klastra wysokiej dostępności:
- Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
- Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn;
- Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera;
- Weryfikacja działania klastra wysokiej dostępności;
- Migracja istniejącej infrastruktury do środowiska wirtualnego;
- Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Konfiguracja powiadomień o krytycznych zdarzeniach (email).

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

6. Serwer backupu – 1 szt.

Urządzenie ma spełniać następujące parametry techniczne, funkcjonalności oraz warunki udzielonej gwarancji producenta:

6.1. Obudowa

- Typu RACK, wysokość nie więcej niż 1U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;
- Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD SATA Hot-Plug 480 GB;
- Zainstalowane 6 szt. dysków SAS/NL-SAS Hot-Plug 2,4 TB.

6.2. Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 86-rdzeniowych;
- Moduł TPM 2.0;
- 32 gniazda pamięci RAM;
- Obsługa 8 TB pamięci operacyjnej RAM DDR4;
- Obsługa pamięci MRDIMM.

6.3. Procesory

Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,3 GHz, architektura x86_64;

6.4. Pamięć RAM

- 64 GB pamięci RAM;
- DDR5 Registered 6400MT/s.

6.5. Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: 4 x 1Gbit Base-T w tym 1 szt. do zarządzania OOB serwerem.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

6.6. Kontrolery RAID

Kontroler SAS RAID obsługujący następujące poziomy RAID: 0,1,10, posiadający wsparcie dla dysków SED.

6.7. Porty

- Zintegrowana karta graficzna ze złączem Display Port;
- 4 porty USB 3.2;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

6.8. Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

6.9. Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
  - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express,
  - procesory CPU,
  - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM,
  - status karty zarządzającej serwera,
  - wentylatory,
  - bateria podtrzymująca ustawienia BIOS płyty głównej,
  - zasilacze;
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
  - niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,
  - dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- dostęp poprzez przeglądarkę Web, SSH,
- zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,
- zarządzanie alarmami (zdarzenia poprzez SNMP),
- możliwość przejęcia konsoli tekstowej,
- przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),
- obsługa serwerów proxy (autentykacja),
- obsługa VLAN,
- możliwość konfiguracji parametru Max. Transmission Unit (MTU),
- obsługa protokołów TLS 1.2,
- obsługa protokołu LDAP,
- synchronizacja czasu poprzez protokół NTP,
- możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;

- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera.

6.10. Wspierane/Certyfikowane OS

- Microsoft Windows Server 2025, 2022;
- VMWare vSphere 9.x,8.x;
- Suse Linux Enterprise Server 15, 16;
- Red Hat Enterprise Linux 9.x, 10.x;
- Oracle Linux 9.x, 10.x;
- XenServer 8.4.

6.11. Gwarancja

- 5 lat gwarancji producenta serwera w trybie on-site w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników;
- 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 (podać koszt na dzień składania oferty).

6.12. Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
- Zgodność z normami: RoHS, WEEE oraz CE.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

7. Biblioteka taśmowa – 1 szt.

Urządzenie ma spełniać następujące parametry techniczne, funkcjonalności oraz warunki udzielonej gwarancji producenta:

Element konfiguracji	Wymagane minimalne parametry techniczne
Wykorzystana technologia	LTO Ultrium wspierająca technologię partycjonowania nośników.
Obudowa	Typu rack 19”. Wysokość maksymalnie 1U - wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem. Urządzenie musi mieć możliwość instalowania w tej samej obudowie różnych generacji napędów LTO (minimum od LTO-6 wzwyż).
Zainstalowany napęd	Jeden napęd LTO-8 wyposażony w dwa złącza mSAS SFF-8088. Urządzenie musi mieć możliwość instalowania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System). Prędkość zapisu napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasety oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2
Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy podzielone na dwa magazynki (urządzenie musi być dostarczone z kompletem magazynków). Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot musi odbywać się bez konieczności wysuwania całego magazynka.
Pojemność	Pojemność bez kompresji – minimum 96TB przy obsadzeniu wszystkich slotów na taśmy wyłącznie nośnikami LTO-8
Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

	podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI
Obsługa urządzenia	Wymagana możliwość wymiany napędu, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki.
Wyposażenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli: 1x zasilając, 1x sieciowy oraz 1x komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabla min. 2m. oraz kontroler SAS do podłączenia biblioteki z posiadanym przez zamawiającego serwerem - interfejs kontrolera: minimum single SAS 12Gb. Wraz z urządzeniem należy dostarczyć także zestaw 6-ciu identycznych nośników na dane o pojemności natywnej pojedynczego nośnika min. 12TB oraz jeden nośnik czyszczący wyposażonych w unikalne naklejki z kodem kreskowym. Wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia dołączonym do oferty – Instrukcja instalacji - w języku polskim lub angielski **L** m
Gwarancja i oświadczenia	36 miesięcy z czasem reakcji do 72 godz. (dni robocze) od momentu zgłoszenia uszkodzenia. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO-9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

8. Oprogramowanie do kopii zapasowych – 1 szt.

Wymagane jest dostarczenie licencji wieczystej na oprogramowanie, z zapewnieniem wsparcia technicznego przez okres do 31.12.2026 r., dla co najmniej 5 maszyn wirtualnych.

8.1. Wymagania ogólne

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

8.2. Całkowite koszty posiadania

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.

Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora).

Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS).

Oprogramowanie musi posiadać integracje z systemami typu SIEM.

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

8.3. Wymagania RPO

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

8.4. Wymagania RTO

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.

8.5. Ograniczenie ryzyka

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.

Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.

Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

8.6. Środowiska fizyczne

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.

Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.

Rozwiązanie musi wspierać system operacyjny macOS

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.

Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).

Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.

Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.

Rozwiązanie musi wspierać backup podłączonych dysków USB.

Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).

Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.

Rozwiązanie musi wspierać kontrolę pasma sieciowego.

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.

Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.

Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.

Rozwiązanie musi wspierać technologię BitLocker.

Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.

Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych.

Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.

Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Rozwiązanie musi wspierać szyfrowanie.

Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.

Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.

Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.

Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

8.7. Monitoring

System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.

System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.

System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.

System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.

System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.

System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.

System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).

System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.

System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.

System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.

System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4.

8.8. Raportowanie

System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.

System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.

System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.

System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.

System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.

System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.

System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.

System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.

System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.

System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.

System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.

System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).

System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

9. Dostawa urządzenia klasy UTM – 1 szt.

System bezpieczeństwa ma realizować 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.ystem 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 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall;
- Ochrony w warstwie aplikacji;
- Protokołów routingu dynamicznego.

9.1. Redundancja, monitoring i wykrywanie awarii

- 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;
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych;
- Monitoring stanu realizowanych połączeń VPN;
- System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

9.2. Interfejsy, dysk, zasilanie

- System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 5 portami Gigabit Ethernet RJ-45;
- System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB;
- System Firewall pozwala skonfigurować co najmniej 20 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q;
- System jest wyposażony w zasilanie AC.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

9.3. Parametry wydajnościowe

- W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę;
- Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B;
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps;
- Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4,3 Gbps;
- 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 Gbps;
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps;
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

9.4. Funkcje Systemu Bezpieczeństwa:

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

- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection;
- Kontrola Aplikacji;
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN;
- Ochrona przed malware;
- Ochrona przed atakami - Intrusion Prevention System;
- Kontrola stron WWW;
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3;
- Zarządzanie pasmem (QoS, Traffic shaping);
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP);
- 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;
- Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3;
- Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- 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).

9.5. Polityki, Firewall

- Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń;
- 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;
- W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN;
- Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP;
- Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe;
- Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna;
- 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.

9.6. Połączenia VPN

- 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),

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- obsługę 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;

- 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.

9.7. Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

- Routingu statycznego;
- Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP);
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM;
- Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu;
- ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu;
- BFD (Bidirectional Forwarding Detection);

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

9.8. Funkcje SD-WAN

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

9.10. Zarządzanie pasmem

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

9.11. Ochrona przed malware

- Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021);
- Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS;
- 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;
- System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów;
- System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android);
- Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
- 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;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików;
- Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta;
- Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

9.12. Ochrona przed atakami

- Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych;
- System chroni przed atakami na aplikacje pracujące na niestandardowych portach;
- Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
- Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur;
- System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS;
- Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty);
- Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
- Wykrywanie i blokowanie komunikacji C&C do sieci botnet;
- Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

9.13. Kontrola aplikacji

- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP;
- Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików;
- Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P;
- Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur;
- Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021);

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- 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).

9.14. Kontrola WWW

- Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne;
- 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;
- Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard;
- Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL;
- Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex);
- Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony;
- Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo;
- Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW;
- System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

9.15. Uwierzytelnianie użytkowników w ramach sesji

- 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;
- System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego;
- 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;
- Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

9.16. Zarządzanie

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

9.17. Logowanie

- 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;
- Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach i funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach) udostępnianej w chmurze lub musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej;
- W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- 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;
- Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa;
- Możliwość włączenia logowania per reguła w polityce firewall;
- System zapewnia możliwość logowania do serwera SYSLOG;
- Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

9.18. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać ICSA lub EAL4 dla funkcji Firewall.

9.19. Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

10. Switch zarządzalny – 1 szt.

Urządzenie ma spełniać następujące parametry techniczne, funkcjonalności oraz warunki udzielonej gwarancji producenta:

Parametr	Minimalne wymaganie
Rodzaj urządzenia	Zarządzalny przełącznik dostępowy przeznaczony do pracy w sieci LAN
Warstwa przełączania	Przełącznik warstwy drugiej
Porty dostępowe	Co najmniej 24 porty 10/100/1000Base-T zakończone złączami RJ45
Porty uplink	Co najmniej 4 porty 10 Gigabit Ethernet SFP+
Port konsolowy	Co najmniej 1 port konsolowy RJ45
Obsługa PoE	Urządzenie bez funkcji zasilania PoE
Przepustowość matrycy przełączającej	Co najmniej 128 Gb/s, liczona w trybie pełnego dupleksu
Wydajność przekazywania pakietów	Co najmniej 190 milionów pakietów na sekundę, liczona w trybie pełnego dupleksu
Tablica adresów MAC	Obsługa co najmniej 32 000 adresów MAC
Opóźnienie przełączania	Nie więcej niż 1 µs dla pakietów o długości 64 bajtów
Liczba obsługiwanych sieci VLAN	Co najmniej 4 000
Rozmiar grupy agregacji łączy	Możliwość agregacji co najmniej 8 portów w ramach jednej grupy
Bufor pakietów	Co najmniej 2 MB
Pamięć operacyjna	Co najmniej 512 MB pamięci DDR3
Pamięć Flash	Co najmniej 64 MB
Obudowa	Obudowa przystosowana do montażu w szafie teleinformatycznej 19”
Wysokość obudowy	Nie więcej niż 1U
Zasilanie	Pojedynczy zasilacz prądu przemiennego AC
Sposób zarządzania	Możliwość pracy samodzielnej oraz centralnego zarządzania z poziomu dostarczonego urządzenia FortiGate za pośrednictwem FortiLink
Automatyczne wdrażanie	Automatyczne wykrywanie, autoryzowanie i konfigurowanie przełącznika z poziomu urządzenia zarządzającego
Centralna konfiguracja	Możliwość centralnego konfigurowania portów, sieci VLAN, agregacji łączy, mechanizmów kontroli dostępu i polityk bezpieczeństwa

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Monitoring	Centralny monitoring stanu urządzenia, portów, połączeń, podłączonych urządzeń oraz wykorzystania interfejsów
Aktualizacja oprogramowania	Możliwość centralnego wykonywania aktualizacji oprogramowania układowego przełącznika
Standard VLAN	IEEE 802.1Q
Agregacja łączy	IEEE 802.3ad/LACP
Protokoły drzewa rozpinającego	Obsługa STP, RSTP oraz MSTP
Uwierzytelnianie dostępu	Obsługa IEEE 802.1X
Wykrywanie urządzeń	Obsługa LLDP oraz LLDP-MED
Kontrola ruchu multicast	Obsługa IGMP Snooping
Ochrona usług DHCP	Obsługa DHCP Snooping
Kontrola dostępu	Obsługa list kontroli dostępu ACL oraz kontroli dostępu zależnej od użytkownika lub urządzenia
Zarządzanie ruchem	Obsługa mechanizmów QoS i priorytetyzacji ruchu
Zarządzanie lokalne	Zarządzanie za pomocą interfejsu graficznego oraz wiersza poleceń
Zarządzanie sieciowe	Obsługa co najmniej HTTPS, SSH i SNMP
Rejestrowanie zdarzeń	Obsługa logowania zdarzeń oraz przekazywania informacji diagnostycznych do systemu centralnego zarządzania
Gwarancja producenta	36 miesięcy

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

11. UPS – 14 szt.

Urządzenie ma spełniać następujące parametry techniczne oraz funkcjonalności:

Parametr	Minimalne wymaganie
Cechy specjalne	System automatycznej regulacji napięcia (AVR) Kompaktowa obudowa typu tower ze standardem HID port USB do automatycznej integracji z popularnymi systemami operacyjnymi, dwa gniazda wyjściowe typu FR
Topologia	Technologia line-interactive
Rodzaj budowy	Model wolnostojący
Wartość znamionowa VA	850 VA
Moc	480 W
Złącze wejściowe	SCHUKO
Długość przewodu wejściowego	1,5 m
Napięcie znamionowe wejściowe	Domyślnie 230 V (220/230/240 V)
Częstotliwość znamionowa	50/60 Hz
Zakres częstotliwości wejściowych	45-63 Hz
Gniazdo	(2) francuskie
Zakres napięcia	230 V
Napięcie znamionowe wyjściowe	230 V
Rodzaj napięcia	AC
Wykres czasu podtrzymywania działania	Pokaż wykres czasu podtrzymania
Zarządzanie akumulatorem	Automatyczny test baterii, ochrona przed głębokim rozładowaniem, zimny start
Parametry znamionowe akumulatora	12 V / 9 Ah

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Rodzaj akumulatora	Szczelne, kwasowo-ołowiowe
Łączność	Port USB (kompatybilny z HID)
Interfejs użytkownika	Wskaźnik LED
Rodzaj interfejsu	Port USB
Wyjściowa moc pozorna	900 VA

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

12. UPS RACK – 1 szt.

Urządzenie ma spełniać następujące parametry techniczne, funkcjonalności oraz warunki udzielonej gwarancji producenta:

Nazwa elementu, parametru lub cechy	**Opis minimalnych wymagań**
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
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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Częstotliwość wyjściowa	50/60 Hz
Współczynnik szczytu	3:1
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	• USB • RS232 DB-9 żeński (HID) • styki przekaźnikowe • miniport wyłącznik ON/OFF • SNMP/Ethernet
Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarczający 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). • Rząd przycisków sterowania • Rząd wskaźników stanu : zasilanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
Sygnały akustyczne	• Awaria • Niski stan naładowania baterii • Przeciążenie • Serwis
Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie) • Przyciski funkcyjne (przewijanie w górę i w dół) • Przycisk Enter (potwierdzający) • Przycisk ON/OFF załączenia i wyłączenia • LED trybu zasilania z sieci (kolor zielony)

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

	• LED trybu baterii (kolor żółty) • LED usterki (kolor czerwony)
Typ obudowy	Uniwersalna Tower/Rack 2U
Dane techniczne karty SNMP	• 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/ • 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. • Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI • Kompatybilność: SNMP v1/v3 i IP v4/v6 • Interfejs: HTML5 • Adresowanie IP: DHCP/BootP/Manualne • Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256 • Dostępny port USB (microUSB - port serwisowy) • Certyfikaty: UL 2900-1, 2900-2-2, IEC 62443-4-2,
Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów operacyjnych.
Maksymalna szerokość	438 mm
Maksymalna głębokość	603 mm
Poziom hałasu w odl. 1m	do 40 dBA dla pracy normalnej
Znaki bezpieczeństwa	CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
Gwarancja producenta	36 miesięcy dla elektroniki, 24 miesiące dla baterii.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

13. Oprogramowanie AV z modułem EDR – 20 szt.

Przedmiotem zamówienia jest dostawa licencji dla 28 końcówek. Minimalne parametry:

13.1. Centralne zarządzanie

- Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS);
- Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim;
- Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania;
- Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS;
- Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID;
- Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory;
- Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji;
- Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej:

  - pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania,

  - pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta,

  - buforowanie ruchu HTTPS;
- Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy;
- Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania;
- Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:

  - Google Authenticator,

  - Microsoft Authenticator,

  - Authy,

  - Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania;
- Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów;
- Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
  - Adresy sieciowe IP,
  - Aktywne zagrożenia,
  - Stan funkcjonowania oraz ochrony,
  - Wersja systemu operacyjnego,
  - Podzespoły komputera.
- Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
  - Wyrażenie CRON,
  - Codziennie,
  - Cotygodniowo,
  - Co miesiąc,
  - Co rok,
  - Po wystąpieniu nowego zdarzenia,
  - Po automatycznym umieszczeniu hosta w grupie dynamicznej.
- Rozwiązanie musi udostępniać możliwość tagowania obiektów;
- Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog;
- Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
  - JSON,
  - LEEF,
  - CEF.

13.2. Ochrona stacji roboczych - Windows

- Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
- Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - Wirus,
  - Trojan,
  - Robak,
  - Adware,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Spyware,
- Dialer,
- Phishing,
- Backdoor.

- Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
- Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
- Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware:
  - Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych,
  - Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service),
  - Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
- Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - Całego dysku,
  - Wybranych katalogów,
  - Pojedynczych plików,
  - Plików spakowanych oraz skompresowanych,
  - Dysków sieciowych,
  - Dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - Wybranych plików,
  - Wybranych procesów,
  - Wybranych lokalizacji,
  - Wybranych rozszerzeń,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Nazwy wykrycia,
- Sumy kontrolnej (SHA1).

- Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
- Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego,
  - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,
  - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- Rozwiązanie musi udostępniać 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 udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
- Rozwiązanie musi udostępniać 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
  a) Typ urządzenia:
     - Pamięci masowe,
     - Optyczne pamięci masowe,
     - Pamięci masowe Firewire,
     - Urządzenia do tworzenia obrazów,
     - Drukarki USB,
     - Urządzenia Bluetooth,
     - Czytniki kart inteligentnych,
     - Modemy,
     - Porty LPT/COM,
     - Urządzenia przenośne,
  b) parametry urządzenia:
     - Numer seryjny,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Producent,

Model.

c) Typ dostępu:

- Brak możliwości zapisu,
- Pełen dostęp,
- Ostrzeżenie użytkownika,
- Brak dostępu.

- Rozwiązanie musi udostępniać moduł HIPS, który 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. 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. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. Raport musi posiadać co najmniej:

  - Listę zainstalowanych aplikacji,
  - Listę usług systemowych,
  - Informacje o systemie operacyjnym i sprzęcie,
  - Listę aktywnych procesów i połączeń sieciowych,
  - Harmonogram systemu operacyjnego,
  - Szczegóły pliku hosts,
  - Informacje o sterownikach.

- Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Antywirus,
- Zapora osobista,
- Sandbox,
- 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 realizowaną przez dedykowaną wtyczkę. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook. Ochrona musi być realizowana w oparciu o co najmniej:
  - globalna czarna lista RBL,
  - czarna lista użytkownika,
  - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
  - Ochrona przed anomaliami sieciowymi, w tym co najmniej:
    - Skanowanie portów TCP oraz UDP,
    - Wykrywanie duplikacji adresu IP,
    - Atak zatruwania ARP,
    - Nieprawidłowa długość pakietu TCP oraz UDP.
  - Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
    - RDP,
    - SMB,
    - My SQL,
    MS SQL,
  - Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
  - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

- Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego. Bezpieczna 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. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
  - Treść komunikatu,
  - Obraz.

13.3. Ochrona stacji roboczych – MacOS

- Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
- Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - Wirus,
  - Trojan,
  - Robak,
  - Adware,
  - Spyware,
  - Dialer,
  - Phishing,
  - Backdoor.
- Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

- Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- Rozwiązanie musi chronić pliki co najmniej za pomocą:
  - Sygnatur wirusów,
  - Reputacji chmurowej.
- Rozwiązanie musi umożliwiać 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 posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu,
  - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,
  - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - całego dysku,
  - wybranych katalogów,
  - pojedynczych plików,
  - plików spakowanych oraz skompresowanych,
  - dysków sieciowych,
  - dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - wybranych plików,
  - wybranych procesów,
  - wybranych lokalizacji,
  - wybranych rozszerzeń,
  - nazwy wykrycia,
  - sumy kontrolnej (SHA1).
- Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego. Zapora osobista musi działać w oparciu o reguły i musi posiadać co

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

najmniej 30 wbudowanych reguł, stworzonych przez producenta. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

- tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący.

13.4. Ochrona stacji roboczych – Linux

- Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
  - Ubuntu Desktop,
  - Red Hat Enterprise Linux,
  - Linux Mint.
- Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
  - Cinnamon.GNOME,
  - KDE,
  - MATE,
  - XFCE.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - Wirus,
  - Trojan,
  - Robak,
  - Adware,
  - Spyware,
  - Dialer,
  - Phishing,
  - Backdoor.
- 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 obu metod jednocześnie.
- Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

- Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - Całego dysku,
  - Wybranych katalogów,
  - Pojedynczych plików,
  - Plików spakowanych oraz skompresowanych,
  - Dysków sieciowych,
  - Dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - Wybranych plików,
  - Wybranych procesów,
  - Wybranych lokalizacji,
  - Wybranych rozszerzeń.
- Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
  - typ urządzenia: pamięci masowe, optyczne pamięci masowe,
  - parametry urządzenia: numer seryjny, producent, model,
  - typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.

13.5. Ochrona serwera – Windows Server

- Rozwiązanie musi wspierać systemy w tym co najmniej:
  - Microsoft Windows Server 2012 R2,
  - Microsoft Windows Server 2016,
  - Microsoft Windows Server 2019,
  - Microsoft Windows Server 2022,
  - Microsoft Windows Server 2025.
- Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - Wirus,
  - Trojan,
  - Robak,
  - Adware.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Spyware,
- Dialer,
- Phishing,
- 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 obu metod jednocześnie.
- Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego,
  - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,
  - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - całego dysku,
  - wybranych katalogów,
  - pojedynczych plików,
  - plików spakowanych oraz skompresowanych,
  - dysków sieciowych,
  - dysków przenośnych.
- 10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - wybranych plików,
  - wybranych procesów,
  - wybranych lokalizacji,
  - wybranych rozszerzeń,
  - nazwy wykrycia,
  - sumy kontrolnej (SHA1).

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- 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. 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. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej. Raport musi posiadać co najmniej:
  - listę zainstalowanych aplikacji,
  - listę usług systemowych,
  - informacje o systemie operacyjnym i sprzęcie,
  - listę aktywnych procesów i połączeń sieciowych,
  - harmonogram systemu operacyjnego,
  - szczegóły pliku hosts,
  - informacje o sterowniku/ach.
- Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
  - antywirus,
  - zapora osobista,
  - sandbox,
  - antyspyware,
  - metody heurystyczne.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

  a) typ urządzenia:
  - Pamięci masowe,
  - Optyczne pamięci masowe,
  - Pamięci masowe Firewire,
  - Urządzenia do tworzenia obrazów,
  - Drukarki USB,
  - Urządzenia Bluetooth,
  - Czytniki kart inteligentnych,
  - Modemy,
  - Porty LPT/COM,
  - Urządzenia przenośne,

  b) parametry urządzenia:
  - Numer seryjny,
  - Producent,
  - Model,

  c) typ dostępu:
  - Brak możliwości zapisu,
  - Pełen dostęp,
  - Ostrzeżenie użytkownika,
  - Brak dostępu.
- Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
  - MS SQL,
  - Active Directory,
  - IIS,
  - Sysvol,
  - DNS,
  - DHCP,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Hyper-V,
- Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

- Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

  a) Ochrona przed anomaliami sieciowymi, w tym co najmniej:
  - Skanowanie portów TCP oraz UDP,
  - Wykrywanie duplikacji adresu IP,
  - Atak zatruwania ARP,
  - Nieprawidłowa długość pakietu TCP oraz UDP.

  b) Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
  - RDP,
  - SMB,
  - My SQL,
  - MS SQL.

  c) Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

- Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
- Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
  - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
  - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
  - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

  Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

13.6. Ochrona serwera – Linux

- Rozwiązanie musi wspierać systemy w tym co najmniej:
  - RedHat Enterprise Linux (RHEL),
  - Rocky Linux,
  - Ubuntu,
  - Debian,

- SUSE Linux Enterprise Server (SLES),
- Oracle Linux,
- Amazon Linux.

- Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
  - Wirus,
  - Trojan,
  - Robak,
  - Adware.
  - Spyware,
  - Dialer,
  - Phishing,
  - Backdoor.
- Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
- 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 obu metod jednocześnie.
- Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
  - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,
  - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
  - całego dysku,
  - wybranych katalogów,
  - pojedynczych plików,
  - plików spakowanych oraz skompresowanych,
  - dysków sieciowych,
  - dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
  - wybranych plików,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- wybranych procesów,
- wybranych lokalizacji,
- wybranych rozszerzeń.

- Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
- Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
- Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
  - proces budowania obrazu kontenera,
  - wdrażanie obrazu kontenera.

13.6. Mobile Device Management

- Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
- MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
  - Android,
  - iOS,
  - iPadOS.
- MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
  - Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
  - Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
  - VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
  - Apple Business Manager (ABM),
  - Android Enterprise (co najmniej w zakresie Device Owner).

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
  - usunięcie zawartości urządzenia,
  - przywrócenie urządzenia do ustawień fabrycznych,
  - zablokowanie urządzenia,
  - uruchomienie sygnału dźwiękowego,
  - lokalizację GPS,
  - Resetowanie hasła blokady ekranu.
- MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- MDM musi umożliwiać co najmniej:
  a) dla systemów iOS oraz iPadOS:
  - konfigurację kont e-mail,
  - konfigurację połączeń VPN,
  - konfigurację połączeń Wi-Fi,
  - konfigurację listy certyfikatów,
  - możliwość uruchomienia trybu jednej aplikacji,

  b) dla systemu Android:
  - blokadę wykonywania połączeń,
  - blokadę konfiguracji sieci Wi-Fi,
  - blokadę konfiguracji tuneli VPN,
  - zarządzenie aktualizacjami sytemu operacyjnego,
  - blokadę zmiany tapety urządzenia.

13.7. Mobile Threat Defense (MTD) dla systemu Android

- Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
- Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
  - Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD,
  - Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
- Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
  a) złożoność kodu blokady ekranu:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Wzór,
- PIN,
- Hasło,

b) przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

c) definiowanie czasu obowiązywania (ważności) kodu blokady ekranu.

- Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
  - nazwę aplikacji,
  - nazwę pakietu,
  - kategorię sklepu Google Play,
  - uprawnienia aplikacji,
  - pochodzenie aplikacji z nieznanego źródła.
- Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

13.8. Sandbox w chmurze

- Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
- Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- Rozwiązanie musi wspierać systemy w tym co najmniej:
  - Microsoft Windows 10 oraz 11,
  - Microsoft Windows Server,
  - macOS 11 (Big Sur) oraz nowszych,
  - RedHat Enterprise Linux (RHEL),
  - Rocky Linux,
  - Ubuntu,
  - Debian,
  - SUSE Linux Enterprise Server (SLES),
  - Oracle Linux,
  - Amazon Linux.
- Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
  - archiwa,
  - skrypty,
  - pliki wykonywalne,
  - pliki rejestru systemowego (.reg),
  - możliwy spam,
  - dokumenty.
- Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
  - natychmiast po ich przeanalizowaniu,
  - po upływie 30 dni,
  - nigdy.
- Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
- Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
- Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
  - czysty,
  - podejrzany,
  - bardzo podejrzany,
  - szkodliwy.
- W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej wstrzymania uruchamiania pobieranych plików z następujących źródeł:
  - przeglądarki internetowe,
  - programy poczty e-mail,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- nośniki wymienne,
- pliki wyodrębnione z archiwum.

- Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

13.9. Szyfrowanie

- Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
- Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
- Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
- W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane. Hasło odzyskiwania nie może być krótsze niż 8 znaków. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
- 7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
- Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
- Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0.
- W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.
- Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia w przypadku aktualizacji systemu operacyjnego.

13.10. Endpoint Detection and Response / eXtended Detection and Response

- Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
  - Tworzenie procesów,
  - Uruchamianie, zatrzymanie i modyfikacja usług,
  - Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,
  - Usuwanie oraz zmiana nazw plików,
  - Tworzenie i usuwanie kluczy rejestru systemowego,
  - Ładowanie bibliotek DLL,
  - Zalogowanie użytkowników,
  - elementy sieciowe, w tym co najmniej: pobranie plików wykonywalnych, zestawienie połączeń TCP/IP, zapytania http, zapytania DNS.
- Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

14. Oprogramowanie do zarządzania infrastrukturą informatyczną – 1 szt.

14.1. Architektura / budowa

- System musi umożliwić bezproblemową i stabilną obsługę co najmniej 40 klientów jednocześnie.
-
- 14.1. **Architektura / budowa**:

  - Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
  - Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
  - Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
  - Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
  - Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.

- Konfiguracja Architektury:

  - Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie,
  - System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

14.2. Wymagania systemowe

- Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
- Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
- Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
- Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition).
- System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

14.3. Interfejsy

- System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
- System zapewnia integrację z modelem LLM.

14.4. Funkcjonalności systemu zarządzania infrastrukturą IT

- Funkcjonalność Klienta. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
- Funkcjonalność konsoli administracyjnej:
  - konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie,
  - w konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

- Funkcjonalność panelu pracownika. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.
- Zarządzanie licencjami. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.
- Wzorce aplikacji i pakietów. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
- Zarządzanie podatnościami:

  - system musi posiadać zdolności do bieżąco i automatycznego identyfikowania podatności w zainstalowanym oprogramowaniu**,**

  - wykrywanie podatności musi być oparte o analizę wzorców zainstalowanego oprogramowania i porównanie ich z globalnymi bazami podatności, takimi jak CVE (Common Vulnerabilities and Exposures),

  - system powinien posiadać co najmniej dwa wskaźniki umożliwiające ocenę poziomu ryzyka i priorytetyzację zagrożeń,

  - system musi mieć możliwość ustawiania powiadomień o wykrytych podatnościach,

  - system musi mieć możliwość automatycznego tworzenia incydentów w przypadku integracji systemu z systemem eHelpDesk,

  - powinna istnieć funkcja raportowanie z możliwością filtrowania wg urządzenia, typu podatności lub poziomu krytyczności.
- Inwentaryzacja sprzętu komputerowego i urządzeń. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.

- Inwentaryzacja urządzeń sieciowych. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
- Inwentaryzacja sprzętu. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
- Ochrona danych (DLP). Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami
- Zdalna administracja komputerami. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
- System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
- System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
- Zdalne Zarządzanie Zaporą (Firewall). System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.
- Automatyzacja. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

- Zarządzanie magazynem IT. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
- Repozytorium. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
- Kody kreskowe. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
- Wysyłanie wiadomości. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
- System musi posiadać możliwość eksportu / importu treści.
- Monitorowanie drukarek sieciowych i wydruków. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
- Monitorowanie stron www. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- Monitorowanie serwerów WWW. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
- Monitorowanie dziennika zdarzeń. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
- System musi umożliwiać monitorowanie komunikatów Syslog.
- Monitorowanie pracy komputerów. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
- Monitorowanie uprawnień ACL. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.
- Monitorowanie sensorów. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
- Repozytorium CMDB. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
- Worktime manager. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.
- Raportowanie i eksport danych. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
- System musi zapewnić interfejs API. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.

- Powiadomienia. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.
- Bezpieczeństwo. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.
- Wsparcie i pomoc. Pomoc techniczna:
  - musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00,
  - utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania,
  - czas trwania usługi SLA do 31.12.2026 r. od dnia zakupu.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

15. Usługa konfiguracji – 1 usługa

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do wykonania niezbędnych czynności wdrożeniowych i konfiguracyjnych, w tym w szczególności:
- przygotowania urządzeń i oprogramowania do pracy w środowisku Zamawiającego,
- instalacji, uruchomienia i podstawowej konfiguracji sprzętu oraz oprogramowania,
- konfiguracji parametrów sieciowych, adresacji, dostępów administracyjnych oraz połączeń z infrastrukturą Zamawiającego,
- konfiguracji polityk bezpieczeństwa, reguł, uprawnień użytkowników i administratorów,
- konfiguracji mechanizmów monitorowania, alertowania, powiadamiania i raportowania,
- integracji wdrażanych urządzeń i rozwiązań z istniejącą infrastrukturą IT/OT/ICS/IIoT Zamawiającego,
- przekazania dokumentacji powykonawczej oraz podstawowego instruktażu dla wskazanych pracowników Zamawiającego.

Celem realizacji usługi jest zapewnienie prawidłowego działania pozostałych elementów infrastruktury cyberbezpieczeństwa, ich dostosowanie do potrzeb Zamawiającego oraz podniesienie poziomu ochrony środowiska IT/OT/ICS/IIoT, w szczególności w zakresie wykrywania zagrożeń, ograniczania ryzyka wystąpienia incydentów, monitorowania infrastruktury, zarządzania dostępem oraz zapewnienia ciągłości działania usług wodociągowych. Dodatkowo przedmiotem zamówienia jest wykonanie usługi wdrożenia i konfiguracji rozwiązań z zakresu cyberbezpieczeństwa dla środowiska IT/OT/ICS/IIoT Zamawiającego, obejmującej uruchomienie, konfigurację oraz integrację centralnego systemu bezpieczeństwa klasy SIEM/CSB wraz z wymaganymi modułami funkcjonalnymi. Wdrożenie oferowanego Centralnego Systemu Bezpieczeństwa (dalej CSB), polegające w szczególności na instalacji oraz uruchomieniu rozwiązania. Do obowiązków Wykonawcy należeć będzie:
- instalacja fizyczna i konfiguracja funkcjonalna komponentów systemu CSB,
- konfiguracja systemu CSB w środowisku Zamawiającego. Zdefiniowanie niezbędnych do poprawnego działania systemu parametrów konfiguracyjnych,
- integracja z usługą katalogową w zakresie autentykacji użytkowników. Konfiguracja ról Użytkowników,
- podłączenie do 3 rodzajów źródeł zdarzeń (np. UTM, switch, serwer) rozpoznawanych przez system CSB. Wykonawca przekaże wytyczne dla Zamawiającego dotyczące koniecznej konfiguracji źródeł zdarzeń Zamawiającego,
- budowa minimum 1 parser dla źródeł zdarzeń nieobsługiwanych automatycznie przez system CSB,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- możliwość tworzenia niestandardowych reguł korelacyjnych/scenariuszy oraz aktywacja/konfiguracja wbudowanych reguł korelacyjnych,
- konfiguracja polityk retencji danych,
- przygotowanie dokumentacji powykonawczej, zawierającej co najmniej zbiór haseł dostępowych, instrukcji i postępowania w razie problemów,
- przygotowanie i przetestowanie procedur kopii bezpieczeństwa i odtwarzania systemu po awarii,
- instalacja najnowszej wersji składników systemu. Efektem wdrożenia musi być działanie CSB (systemu klasy SIEM) w środowisku IT Zamawiającego.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

16. Dostawa i wdrożenie systemu zabezpieczeń sieciowych i monitorowania cyberzagrożeń w obszarze OT – 1 szt.

Przedmiotem zamówienia jest wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS):

- dostawa licencji oraz sond sprzętowych,
- udzielenie wsparcia dla administratorów Zamawiającego,
- organizacja i realizacja szkoleń dla administratorów Zamawiającego.

16.1. Funkcjonalność i specyfikacja.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:

- pasywne monitorowanie sieci przemysłowej Zamawiającego,
- automatyczne tworzenie graficznej mapy rządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- szczegółową inwentaryzację urządzeń,
- automatyczne odzwierciedlenie połączeń komunikacyjnych,
- informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
- wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
- budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
- obsługę LLDP, CDP, CIP, SSDP.

10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line” przy wpięciu do linii.
15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)
20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC-

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

61850, SRTP, BACnet.

26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.

27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.

28. System IDS musi wykrywać zagrożenia min.:

- malware/”zero-day”,
- atak DOS/DDOS,
- atak typu ATP,
- spyware, skanowanie sieci,
- zagrożenia Man-in-the-Middle,
- anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
- wykrywanie połączeń do innej sieci LAN/internet,
- wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.

29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.

30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.

31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.

32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.

33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.

34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BORADCAST.

35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.

36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.

37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.

38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.

39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.

40. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.

41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.

42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
45. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
49. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
50. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
51. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

16.2. Dostawa, wdrożenie.

1. Wykonawca dostarczy:
   - sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
   - licencję wieczystą na system IDS dla co najmniej 500 szt monitorowanych urządzeń.

2. Usługi wsparcia serwisowego producenta systemu IDS na okres do 31.12.2026 r. serwis producenta systemu IDS ma obejmować:
   - dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim,
   - dostęp do nowych wersji systemu IDS,
   - dostęp do aktualizacji i poprawek systemu IDS,
   - dostęp do aktualizacji oprogramowania sond sprzętowych,
   - wymianę uszkodzonych sond sprzętowych w razie awarii,
   - przekazanie danych kontaktowych do działu technicznego producenta systemu IDS,
   - wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji,
   - wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
3. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
4. Licencje systemowe oraz sprzęt serwerowy zapewni Zamawiający.
5. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.

6. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.

7. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.

8. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.

9. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.

10. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.

11. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU