Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia

Spis treści

1. CENTRALNY SYSTEM BEZPIECZEŃSTWA

WYMAGANIA MINIMALNE:

1.1. LICENCJA

1.1.1.1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć oprogramowanie klasy SIEM (oprogramowanie Systemu Bezpieczeństwa, dalej SB) wraz z licencją bezterminową.

1.1.1.2. Oprogramowanie musi posiadać wsparcie do dnia 30.06.2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

1.1.1.3. Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

1.1.1.4. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

1.2. WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

1.2.1.1. 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.

1.2.1.2. 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 w ilości 95 urządzeń końcowych.

1.2.1.3. 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.

1.2.1.4. Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).

1.2.1.5. Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.

1.2.1.6. Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.

1.2.1.7. Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.

1.2.1.8. Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.

1.2.1.9. 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.

1.2.1.10. Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

1.2.1.11. Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).

1.2.1.12. Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.

1.2.1.13. Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

1.2.1.14. Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.

1.2.1.15. Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.

1.2.1.16. Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.

1.2.1.17. Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie.

1.2.1.18. 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.

1.2.1.19. Zgodność ze standardami HTML i CSS całego serwisu www.

1.2.1.20. Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA.

1.2.1.21. 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.

1.2.1.22. System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

1.3. MODUŁ ANALIZY PODATNOŚCI

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

1.3.1.1.1. 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.

1.3.1.1.2. 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.

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

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

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

1.3.1.3.1. 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).

1.4. MODUŁ MONITORINGU ZASOBÓW

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

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

1.4.1.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami.

1.4.1.2.1. 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.

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

1.4.1.3.1. 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.

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

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

powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: “help-desk”, przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

1.4.1.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej.

1.4.1.5.1. 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).

1.4.1.6. Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT.

1.4.1.6.1. 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.

1.4.1.7. Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT.

1.4.1.7.1. 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.

1.4.1.8. Zdalny dostęp do urządzeń końcowych.

1.4.1.8.1. 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.

1.4.1.9. Wywoływanie predefiniowanych skryptów na urządzeniach końcowych.

1.4.1.9.1. 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.

1.4.1.10. Analiza ruchu sieciowego.

1.4.1.10.1. 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.

1.4.1.11. Monitorowanie problemów i zdarzeń występujących na drukarkach.

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

1.5. MODUŁ ANALIZY LOGÓW

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

1.5.1.1.1. 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.

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

1.5.1.2.1. 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.

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

1.5.1.3.1. 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.

1.5.1.4. Przegląd i analiza logów dotyczących działań użytkowników.

1.5.1.4.1. 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.

1.5.1.5. Dostęp do logów historycznych.

1.5.1.5.1. 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.

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

1.5.1.6.1. 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.

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

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

1.6. MODUŁ EDR/XDR

1.6.1.1. 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.

1.6.1.2. 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.

1.6.1.3. 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.

1.7. MODUŁ INWENTARYZACJI

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

1.7.1.1.1. 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.

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

1.7.1.2.1. 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.

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

1.7.1.3.1. 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.

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

1.8.1.1. Integracja z systemem tiketowym.

1.8.1.1.1. 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.

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

1.8.1.2.1. 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.

1.8.1.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

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

1.9. MODUŁ WYKRYWANIA ZAGROŻEŃ

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

1.9.1.1.1. 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.

1.9.1.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń.

1.9.1.2.1. 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.

1.9.1.3. Historia wykrytych zagrożeń.

1.9.1.3.1. 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).

1.9.1.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia.

1.9.1.4.1. 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.

1.10. MODUŁ RAPORTÓW

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

1.10.1.1.1. 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.

1.11. PANEL UŻYTKOWNIKA

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

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

1.11.1.2. Wizualizacja statystyk zdarzeń i logów.

1.11.1.2.1. 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.

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

1.11.1.3.1. 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).

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

1.11.1.4.1. 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.

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

1.11.1.5.1. Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi

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

1.12. MODUŁ ANALIZY DANYCH AI

1.12.1.1. 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.

1.12.1.2. Analiza bieżących logów.

1.12.1.2.1. 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.

1.12.1.3. Analiza wykrytych zagrożeń.

1.12.1.3.1. 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.

1.12.1.4. Analiza problemów.

1.12.1.4.1. 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.

1.13. MODUŁ THREAT INTELLIGENCE

1.13.1.1. 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.

1.13.1.2. Lista wskaźników – MALWARE.

1.13.1.2.1. 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.

1.13.1.3. Lista wskaźników – zagrożenia sieciowe.

1.13.1.3.1. 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.

1.13.1.4. Lista wskaźników – złośliwe adresy URL.

1.13.1.4.1. 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, 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.

1.13.1.5. Lista blokowanych plików.

1.13.1.5.1. 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.

1.13.1.6. Wyszukiwanie i filtrowanie.

1.13.1.6.1. 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.

1.14. MODUŁ UEBA

1.14.1.1. 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.

1.14.1.2. Predefiniowane reguły wykrywania anomalii UEBA.

1.14.1.2.1. 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:

1.14.1.2.1.1. 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,

1.14.1.2.1.2. 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,

1.14.1.2.1.3. 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,

1.14.1.2.1.4. 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,

1.14.1.2.1.5. podejrzanych logowań lub eskalacji uprawnień, reguła musi wykrywać anomalie, w zachowaniach takich jak logowania z nieznanych lokalizacji lub kont o wysokich uprawnieniach.

1.14.1.3. Parametryzacja i trenowanie zaimplementowanych modeli ML.

1.14.1.3.1. 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.

1.14.1.4. Prezentacja i wizualizacja wykrytych anomalii.

1.14.1.4.1. 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.

1.14.1.5. Wektor ataku.

1.14.1.5.1. System musi być wyposażony w funkcjonalność umożliwiającą wybranie zgłoszonej anomalii i sprawdzenie jak potencjalne zagrożenie przebiegało w infrastrukturze IT. Wektor ataku powinien być przedstawiony w postaci interaktywnej mapy sieci, przedstawiającej te elementy infrastruktury, przez które przeszedł potencjalny cyberatak.

1.14.1.6. Wyszukiwanie i filtrowanie.

1.14.1.6.1. 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.

1.15. MODUŁ OBSŁUGI ZGŁOSZEŃ

1.15.1.1. System musi posiadać 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.

1.15.1.2. Moduł obsługi zgłoszeń musi posiadać 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.

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

1.16. MODUŁ SYMULACJI ATAKU

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

1.16.1.2. Scenariusze ataków.

1.16.1.2.1. 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.

1.16.1.3. Symulacje ataków.

1.16.1.3.1. 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).

1.17. MODUŁ SLA

1.17.1.1. 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.

1.17.1.2. Ustawienia SLA.

1.17.1.2.1. 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 być 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.

1.17.1.3. Lista zdarzeń dla podatności CVE.

1.17.1.3.1. 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.

1.17.1.4. Lista zdarzeń dla problemów.

1.17.1.4.1. 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.

1.17.1.5. Lista zdarzeń dla zagrożeń.

1.17.1.5.1. 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 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.

1.17.1.6. Lista Incydentów EDR.

1.17.1.6.1. 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.

2. UPS

2.1.1.1. Moc pozorna: minimum 20kVA

2.1.1.2. Moc rzeczywista: minimum 20kW

2.1.1.3. Technologia: on-line (VFI), podwójna konwersja

2.1.1.4. Sprawność przy pracy sieciowej: minimum 96 %

2.1.1.5. Typ obudowy: tower

2.1.1.6. Możliwość pracy w konfiguracji fazowej: 3/3, 3/1, 1/1

2.2. Wejście

2.2.1.1. Zakres napięcia wejściowego: minimum 138-485(L-L)

2.2.1.2. Zakres częstotliwości : minimum 40-70 Hz

2.2.1.3. Czas przełączania sieć – bateria: 0ms

2.2.1.4. Współczynnik odkształceń prądu wejściowego THDi: ≦ 3 % (przy pełnym obciążeniu)

2.3. Wyjście

2.3.1.1. Napięcie wyjściowe: 380VAC/400VAC/415 VAC

2.3.1.2. Częstotliwość napięcia wyjściowego: 50/60 Hz ± 0,1Hz

2.3.1.3. Kształt napięcia wyjściowego: sinusoidalny

2.3.1.4. Współczynnik odkształceń prądu wejściowego THD: ≦ 2 % (obciążenie liniowe); ≦ 4 % (obciążenie nieliniowe)

2.3.1.5. Baterie w wewnątrz obudowy UPS / w zewnętrznym zamkniętym MODULE BATERYJNYM: minimum 12V; szczelne, bezobsługowe, o projektowanej żywotności w temperaturze 20 *C minimum 6-8 lat wg Eurobat

2.3.1.6. Czas podtrzymania dla obciążenia 15kW: minimum 15 minut

2.4. Pozostałe

2.4.1.1. Prąd ładowania baterii (wartości ustawiane): minimum 1-10A

2.4.1.2. Wejście zasilania: listwa zaciskowa / terminal śrubowy

2.4.1.3. Wyjście zasilania: listwa zaciskowa / terminal śrubowy

2.4.1.4. Przeciążalność w trybie sieciowym AC: 105%~110%: 60min; 110%~130%: 15min; 130%~155%: 1min

2.4.1.5. Sygnalizacja: Dotykowy wyświetlacz LCD minimum 4,3" z menu w języku polskim

2.4.1.6. Informacje wyświetlane na panelu LCD - wartości minimalne:

- Napięcie wejściowe i wyjściowe
- Częstotliwość wejściowa lub wyjściowa
- Praca w trybie sieciowym, bateryjnym, bypass
- Aktualne obciążenie
- Napięcie na akumulatorach
- Prąd ładowania i rozładowania akumulatorów
- Pozostały czas pracy na akumulatorach (w minutach)

2.4.1.7. Diody LED - dwukolorowe, informujące o poprawnej lub niepoprawnej pracy - wartości minimalne:

- praca AC/DC
- praca DC/AC
- praca w trybie BYPASS
- praca bateryjna/niski poziom naładowania baterii
- przeciążenie

2.4.1.8. Zabezpieczenia - wartości minimalne:

- Zabezpieczenie przed zwarciem na wyjściu
- Zabezpieczenie przed przepięciem na wejściu
- Zabezpieczenie przed przeciążeniem
- Zabezpieczenie przez zbyt wysoką temperaturą
- Zabezpieczenie przed zbyt niskim napięciem akumulatorów

2.4.1.9. Bezpieczniki: minimum 4 - wejście, bypass, wyjście, bypass serwisowy

2.4.1.10. Zimny Start: wymagany

2.4.1.11. Ustawiany czas zwarcia: minimum 10-200ms

2.4.1.12. Funkcja usuwania pyłu wewnątrz UPS poprzez ręczne załączenie wentylatorów: wymagane

2.4.1.13. Interfejsy komunikacyjne / złącza: RS485, SNMP

2.4.1.14. Programowalne styki bezpotencjałowe : minimum 1 wejściowe i 4 wyjściowe

2.4.1.15. Ilość ustawień dla styków bezpotencjałowych: minimum 6 dla wejścia i 13 dla wyjścia

2.4.1.16. Zewnętrzny, bezprzerwowy bypass serwisowy tego samego producenta co UPS, 3-przełącznikowy dający możliwość założenia mechanicznego zabezpieczenia na każdym z rozłączników, w każdej z dwóch domyślnych pozycji (załączony/rozłączony): wymagany

2.4.1.17. Praca równoległa do 4 urządzeń: wymagana

2.4.1.18. Waga UPS (z bateriami): do 150 kg

2.4.1.19. Waga Modułu Bateryjnego z bateriami (jeżeli występuje): do 290 kg

2.4.1.20. Wymiary UPS: nie większe niż: wysokość 885 mm, szerokość 310 mm, głębokość 805 mm

2.4.1.21. Wymiary Modułu Bateryjnego (jeżeli występuje): nie większe niż: wysokość 890 mm, szerokość 320 mm, głębokość 820 mm

2.4.1.22. Poziom hałasu: < 55 dB

2.4.1.23. Temperatura pracy (*C): od -5 do +40

2.4.2. Gwarancja:

- minimum 24 miesiące na elektronikę i 12 miesięcy na akumulatory;

2.4.3. Serwis:

- autoryzowany serwis producenta zlokalizowany w Polsce.
- naprawa w maksymalnie 14 dni roboczych

- serwis realizowany w systemie onsite - w miejscu instalacji sprzętu
- gwarancja realizowana wyłącznie przez Autoryzowany Serwis Producenta

2.4.4. Oprogramowanie:

- oprogramowanie w języku angielskim lub polskim do zarządzania i monitorowania pracy UPS
- wsparcie dla systemów: Windows, Linux

2.5. USŁUGI

2.5.1.1. Dostawa do poziomu zero bez wniesienia, montaż BYPASS (w odległości nie większej niż 3m od UPS), podłączenie BYPASS (do instalacji elektrycznej Zamawiającego, podłączenie BYPASS do UPS, podłączenie UPS/MODUŁU, pierwsze uruchomienie, szkolenie z obsługi.

2.6. DODATKOWE INFORMACJE

2.6.1.1. Spełnione normy: minimum EN IEC 62040-1, EN IEC 62040-2, EN 62040-3

2.6.1.2. Deklaracje zgodności: minimum CE

3. System Backup-rozbudowa

3.1. Typ rozwiązania

3.1.1.1. Kompleksowe rozwiązanie przeznaczone do centralnego tworzenia kopii zapasowych różnych systemów i ich bezpiecznego przechowywania.

3.1.1.2. Wymagane jest, aby oferowane rozwiązanie pochodziło od jednego producenta i było dedykowanym systemem przeznaczonym tylko i wyłącznie do backupu.

3.1.1.3. Nie zezwala się na oferowanie serwerów fizycznych z systemami operacyjnymi oraz dodatkowym oprogramowaniem do wykonywania kopii zapasowych.

3.2. Obudowa

3.2.1.1. Typu desktop – obudowa wolnostojąca.

3.3. Procesor

3.3.1.1. Jeden procesor osiągający wynik minimum 3000 punktów w teście PassMark.

3.4. Pamięć RAM

3.4.1.1. Minimum 16GB w dowolnej konfiguracji modułów pamięci.

3.5. Dołączone dyski

3.5.1.1. Minimum 4 dyski 3.5” HDD o pojemności minimum 8TB każdy zgodne z listą kompatybilności oferowanego rozwiązania oraz charakteryzujące się następującymi parametrami:

- interfejs: SATA 6Gb/s,
- prędkość obrotowa: minimum 7200 RPM,
- MTBF: minimum 1 milion,
- możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego rozwiązania bez potrzeby demontażu dysku.

3.5.1.2. Minimum 2 dyski M.2 NVMe o pojemności minimum 400GB każdy zgodne z listą kompatybilności oferowanego rozwiązania oraz charakteryzujące się następującymi parametrami:

- interfejs: M.2 NVMe PCIe 3.0 x4,
- odczyt losowy (4 KB, QD256): do 220 tysięcy IOPS,
- zapis losowy (4 KB, QD256): do 40 tysięcy IOPS,
- wytrzymałość (TBW): minimum 450TB,
- MTBF: minimum 1,5 miliona,
- możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego rozwiązania bez potrzeby demontażu dysku.

3.6. Interfejsy sieciowe

3.6.1.1. Minimum:

3.6.1.1.1. • 1 port 1GbE RJ-45 (zarządzanie),

3.6.1.1.2. • 1 port 10GbE RJ-45 (przesyłanie danych).

3.7. Obsługa RAID

3.7.1.1. Minimum:

3.7.1.1.1. • Automatyczna konfiguracja dysków HDD w RAID 5 oraz dysków SSD w RAID 1,

3.7.1.1.2. • Możliwość wymiany dysków podczas pracy urządzenia.

3.8. System plików

3.8.1.1. System plików BTRFS lub równoważny.

3.9. Przestrzeń

3.9.1.1. Dostępna przestrzeń użytkowa nie mniejsza niż 14 TB.

3.10. Język GUI

3.10.1.1. Polski lub angielski.

3.11. Usługi backupu

3.11.1.1. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 10 lub nowszym oraz serwerów z systemem Windows Server 2019 lub nowszym według zdefiniowanego planu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich retencją w sposób automatyczny poprzez dedykowany algorytm. Wymagane jest włączenie deduplikacji globalnej po stronie źródła. Połączenie agenta kopii zapasowej (PC, serwery fizyczne) z serwerem kopii zapasowej nawiązywane za pomocą klucza połączenia bez konieczności stosowania nazwy użytkownika i hasła.

3.11.1.2. Wykonywanie kopii zapasowych maszyn wirtualnych ze środowisk takich jak VMware vSphere, VMware free ESXi oraz Microsoft Hyper-V (wraz z klastrami przełączania awaryjnego) z wykorzystaniem centralnego panelu zarządzania oraz dodatkowo:

- obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK,

- obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0,
- kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu,
- kopia zapasowa bez agentów,
- korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej,
- przywracanie całego urządzenia, przywracanie na poziomie plików lub folderów oraz natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub lub wbudowanej platformy wirtualizacji.
- kopia zapasowa uwzględniające aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V.

3.11.1.3. Wykonywanie kopii zapasowych baz danych Microsoft SQL Server i Oracle Database, poprzez kopie zapasowe całych serwerów fizycznych i maszyn wirtualnych. Obsługa pobierania na poziomie plików i baz danych/instancji, przywracając całe serwery fizyczne i maszyny wirtualne z możliwością szybkiego dostęp do tabel i danych dzięki natychmiastowemu przywracaniu do VMware, Hyper-V lub wbudowanej platformy wirtualizacji.

3.11.1.4. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania lub na etapie wykonywania kopii zapasowej po stronie źródła.

3.11.1.5. Licencja musi umożliwiać podłączanie kolejnych komputerów, maszyn wirtualnych i serwerów fizycznych do systemu kopii zapasowej bez limitu podczas okresu ważności gwarancji, wsparcia oraz po zakończeniu tego okresu.

3.12. Bezpieczeństwo

3.12.1.1. Wymagana obsługa WORM, czyli możliwości włączenia ochrony danych kopii zapasowej, objętych wybranym planem ochrony, przed nieautoryzowanymi zmianami i usunięciem (tryb niezmienności – WORM).

3.13. Zasilacz

3.13.1.1. Pojedynczy zasilacz zewnętrzy (adapter) lub wewnętrzy (micro ATX).

3.14. Certyfikaty

3.14.1.1. Minimum:

- CE,
- Zgodność z dyrektywą RoHS.

3.15. Gwarancja

3.15.1.1. Minimum 60 miesięcy gwarancji.

4. Serwer – Typ 1

4.1. Obudowa

4.1.1.1. Obudowa Rack o wysokości 1U.

4.1.1.2. 8 slotów na dyski 2.5”.

4.1.1.3. Możliwość instalacji dysków SAS/SATA – Fabryczna blokada demontowania dysków twardych za pomocą zamka lub linki zabezpieczającej lub innego podobnego zabezpieczenia.

4.1.1.4. LCD na froncie obudowy lub diody LED informujące o stanie komponentów np. CPU, RAM, SSD, zasilanie.

4.2. Płyta główna

4.2.1.1. Płyta główna w architekturze dwuprocesorowej z możliwością zainstalowania procesorów 64 rdzeniowych.

4.2.1.2. Płyta główna musi umożliwiać instalacje minimum 32 kości DDR5 z możliwością wyskalowania pamięci do minimum 8TB.

4.3. Procesor

4.3.1.1. Zainstalowane procesor, dedykowane do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 379 w teście SPECrate2017_fp_base w konfiguracji jedno lub dwuprocesorowej, dostępnym na stronie www.spec.org.

4.4. RAM

4.4.1.1. 128GB DDR5 RDIMM 5600MHz.

4.4.1.2. Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC.

4.5. Kontroler RAID

4.5.1.1. Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID 0, 1, 10, 5, 6, 50, 60. Wyposażony w 4GB pamięci podręcznej podtrzymywanej bateryjnie.

4.6. Dyski twarde

4.6.1.1. Zainstalowane:

- 3x dysk SSD SATA o pojemności min. 1,92TB

4.6.1.2. Wsparcie dla dysków M.2 SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

4.7. Gniazda PCIe

4.7.1.1. 2x PCIe 4.0 16X

4.8. Interfejsy sieciowe/FC/SAS

4.8.1.1. Min. 2 interfejsy sieciowe 1GB (interfejsy nie mogą zajmować slotów PCIe)

4.8.1.2. Min. 2 interfejsy sieciowe 10GBASE-T

4.9. Wbudowane porty oraz wskaźniki

4.9.1.1. 5 portów USB w tym min:

- 2 porty USB 3.0 z tyłu obudowy,
- 2 port USB 3.0 z przodu obudowy
- 1 port USB 2.0 zainstalowany wewnętrznie

4.9.1.2. 2 porty VGA

4.9.1.3. 2 dedykowane, wbudowane poty umożliwiające zarządzanie serwerem, z czego co najmniej jeden umożliwiający połączenie z graficznym interfejsem zarządzającym, przynajmniej jeden port na przodzie obudowy umożliwiający połączenie za pomocą USB Type-C.

4.9.1.4. Przyciski i wskaźniki:

- Diagnostyczny panel LED – panel musi wyświetlać informacje na temat aktualnego stanu serwera. W przypadku awarii, panel LED musi wskazywać odpwiedni kod błędu, a w sytuacji wystąpienia więcej niż jednego błędu, system musi wyświetlać odpowiednie kody błędów w pętli.

- Wskaźnik aktualnego stanu urządzenia – wskaźnik musi za pomocą stosownego koloru oraz określonej czestotliwości odświeżania wyświetlać w jakim stanie znajduje się urządzenie.

- Wskaźnik stanu karty OCP NIC. Wskaźnik musi informować czy:

  a) Karta została wykryta

  b) Karta została wykryta ale nie jest włączona

  c) Karta została zainstalowana, wykryta i działa poprawnie

- Wskaźnik stanu zasilania zintegrowany z przyciskiem zasilania informujący czy:

  a) Urządzenie jest włączone.

  b) Urządzenie jest wyłączone.

  c) Urządzenie zostało uruchomione, a moduł zarządzania się uruchamia. W tej sytuacji wciśnięcie przycisku zasilania nie może spowodować wyłączenia serwera.

- Wskaźnik UID zintegrowany z przyciskiem, umożliwiający zlokalizowanie urządzenia, udostępniający następnujące funkcje:

  a) Przycisk migający lub świecący ciągłbym swiatłem niebieskim umożliwia zlokalizowanie serwera.

  b) Włączenie/wyłączenie funkckcji lokalizacji urządzenia musi być możliwe zarówno z poziomu przycisku jak i z poziomu interfejsu zarządzania.

- Wskaźnik statusu bezpośredniego połączenia z interfejsem zarządzania. Musi informować o aktualnym stanie połączenia z

interfejsem zarządzania umieszczonym na przednim panelu urządzenia.

4.9.1.5. Wszystkie wskaźniki oraz porty muszą znajdować się na przodzie urządzenia co znacząco ułatwi analizę wyświetlanych komunikatów. Sam sposób wyświetlania informacji musi być opisany w dokumentacji, a ich funkcje muszą być zgodnie z obowiązującymi praktytami w tym zakresie.

4.10. Video

4.10.1.1. Zintegrowana karta graficzna z minimum 32MB pamięci osiągająca rozdzielczość 1920x1200 60Hz

4.11. Wentylatory

4.11.1.1. Redundantne

4.12. Zasilacze

4.12.1.1. Minimum dwa redundantne zasilacze o mocy minimum 900W z certyfikatem minimum Titanium.

4.12.1.2. Elementy montażowe Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych

4.13. Bezpieczeństwo

4.13.1.1. Moduł TPM 2.0

4.13.1.2. Secure boot

4.13.1.3. Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera.

4.14. Moduł zarządzania

4.14.1.1. Niezależny od zainstalowanego na serwerze systemu operacyjnego, moduł zarządzania, posiadająca dedykowany port Gigabit Ethernet RJ45.

4.14.1.2. NC-SI

4.14.1.3. Zarządzanie certyfikatami. Moduł musi obsługiwać szyfrowanie i wymianę certyfikatów SSL. Wymiana samych certyfikatów musi być możliwa z poziomu GUI.

4.14.1.4. Moduł musi umożliwiać import certyfikatu LDAP (Lightweight Directory Access Protocol.

4.14.1.5. Wsparcie dla DCMI 1.5.

4.14.1.6. Wsparcie dla IMPI 1.5 oraz 2.0.

4.14.1.7. Moduł zarządzania musi posiadać certyfikacje CC EAL4+.

4.14.1.8. Wymagana jest funkcjonalność zarządzania diagnostyką błędów (FDM. Funkcjonalność musi obejmować zbieranie i analizę danych o błędach, diagnozowanie i lokalizowanie błędów, wczesne ostrzeganie o błędach oraz analizę kondycji urządzeń. Podczas rutynowej obsługi i konserwacji można wyświetlać informacje o wadliwych komponentach oraz związanych z nimi zdarzeniami historycznymi. Wymagana funkcjonalność musi być możliwa do włączenia/wyłączenia z poziomu BIOS.

4.14.1.9. Moduł musi oferować precyzyjne powiadomienia o niekrytycznych, niekorygowalnych błędach (UCE) w pamięci w sposób umożliwiający zlokalizowanie uszkodzonego modułu.

4.14.1.10. Wymagana jest obsługa szczegółowych alarmów dotyczących dysków twardych, które mogą rozróżniać trzy typy alarmów: oprogramowania układowego dysku twardego, konfigurację i usterki fizyczne.

4.14.1.11. Musi umożliwiać przeglądanie w formie graficznego modelu 3D rozkładu temperatury. Mapa temperatury musi umożliwić lokalizowanie anomalii związanych z temperaturą wewnątrz urządzenia w dowolnym jego punkcie.

4.14.1.12. Moduł musi umożliwiać włączenie funkcji szyfrowania KVM i VNC (Virtual Network Console), które szyfrują dane przesyłane do i z zdalnej konsoli wirtualnej.

4.15. BIOS

4.15.1.1. Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności:

4.15.1.2. Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.

4.15.1.3. Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.

4.15.1.4. Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu.

4.15.1.5. Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware'u oraz zapewniać wsparcie dla aktualizacji zdalnych.

4.16. System do zarządzania serwerem

4.16.1.1. Oferowany serwer musi być wyposażony w zaawansowane oprogramowanie do zarządzania i monitorowania, które umożliwia centralne zarządzanie oraz optymalizację pracy serwera. Oprogramowanie musi spełniać następujące wymagania:

4.16.2. Centralne zarządzanie serwerami

4.16.2.1. Oprogramowanie do zarządzania serwerami musi zapewniać:

4.16.2.1.1. Monitorowanie infrastruktury w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wydajności serwerów, stanu komponentów oraz zużycia zasobów, prezentując dane w formie graficznej.

4.16.2.1.2. Automatyzacja aktualizacji: Musi wspierać zdalne i automatyczne aktualizowanie oprogramowania układowego oraz sterowników, z możliwością planowania aktualizacji.

4.16.2.1.3. Diagnostyka i analiza stanu sprzętu: System musi umożliwiać analizę kondycji serwerów, gromadząc dane diagnostyczne i identyfikując potencjalne problemy przed ich wystąpieniem.

4.16.2.1.4. Zarządzanie wieloma serwerami jednocześnie: Oprogramowanie musi umożliwiać zarządzanie co najmniej 50 serwerami z jednej platformy zarządzającej.

4.16.3. Moduł zarządzania płytą główną

4.16.3.1. Serwer musi być wyposażony w moduł zarządzania, który oferuje następujące funkcjonalności:

4.16.3.1.1. Dostęp do zdalnej konsoli serwera: Moduł musi umożliwiać pełną kontrolę nad serwerem poprzez zdalny dostęp do konsoli, niezależnie od stanu systemu operacyjnego.

4.16.3.1.2. Monitorowanie sprzętu: Moduł musi zapewniać monitorowanie parametrów sprzętowych, takich jak temperatura, prędkość wentylatorów, napięcia oraz stan kluczowych komponentów.

4.16.3.1.3. Obsługa wirtualnych nośników: Moduł musi umożliwiać montowanie obrazów dysków zdalnie, co ułatwia instalację systemów operacyjnych oraz aktualizacje oprogramowania.

4.16.3.1.4. Bezpieczne zarządzanie: Moduł musi wspierać szyfrowanie komunikacji oraz integrację z systemami uwierzytelniania, takimi jak LDAP, oraz zarządzanie certyfikatami.

4.16.3.1.5. Wsparcie dla standardowych protokołów zarządzania: Moduł musi obsługiwać popularne protokoły zarządzania sprzętem, umożliwiając integrację z zewnętrznymi systemami zarządzania.

4.16.4. System zarządzania zasobami serwera

4.16.4.1. Serwer musi być wyposażony w oprogramowanie do zarządzania zasobami, które zapewnia:

4.16.4.1.1. Monitorowanie obciążenia w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wykorzystania procesora, pamięci oraz przestrzeni dyskowej, prezentując dane w formie wykresów i raportów.

4.16.4.1.2. Automatyczna optymalizacja zasobów: System musi posiadać funkcję automatycznego dostosowywania przydziału zasobów, aby maksymalizować wydajność serwera.

4.16.4.1.3. Zarządzanie cyklem życia sprzętu: Oprogramowanie musi wspierać planowanie konserwacji, aktualizacje oprogramowania układowego oraz zarządzanie konfiguracją serwera.

4.16.4.1.4. Integracja z zewnętrznymi systemami zarządzania: System musi obsługiwać standardowe interfejsy API, co umożliwia integrację z narzędziami do automatyzacji i zarządzania infrastrukturą.

4.16.5. Oprogramowanie do zarządzania serwerem lokalnie i zdalnie

4.16.5.1. Oferowane oprogramowanie musi umożliwiać zarządzanie serwerami zarówno lokalnie, jak i zdalnie, zapewniając:

4.16.5.1.1. Automatyzację konfiguracji i monitorowania: Oprogramowanie musi umożliwiać automatyczną konfigurację serwerów, monitorowanie ich stanu oraz zarządzanie zasobami.

4.16.5.1.2. Integrację z popularnymi platformami chmurowymi: Musi wspierać integrację z rozwiązaniami używanymi w środowiskach chmurowych, takimi jak narzędzia do wirtualizacji oraz systemy zarządzania centrami danych.

4.16.5.1.3. Monitorowanie zużycia energii: Oprogramowanie musi oferować funkcje monitorowania zużycia energii oraz zarządzania profilami energetycznymi serwerów, co pozwala na optymalizację kosztów energii.

4.16.6. Otwarte standardy zarządzania sprzętem

4.16.6.1. Oprogramowanie musi wspierać otwarte standardy zarządzania sprzętem, takie jak nowoczesny interfejs API, który zapewnia:

4.16.6.1.1. Zdalne zarządzanie sprzętem: API musi umożliwiać programistyczne zarządzanie serwerem, monitorowanie jego parametrów oraz automatyzację zadań administracyjnych.

4.16.6.1.2. Bezpieczną komunikację: API musi wspierać szyfrowanie danych oraz integrację z narzędziami do zarządzania certyfikatami.

4.16.6.2. Integrację z narzędziami do automatyzacji: API musi umożliwiać integrację z popularnymi narzędziami automatyzacji, takimi jak systemy zarządzania konfiguracją i orkiestracji.

4.17. Wymagania dotyczące systemu diagnostycznego

4.17.1.1. Oferowany serwer musi być wyposażony w zaawansowany system diagnostyczny, który zapewnia kompleksowe monitorowanie stanu sprzętu oraz precyzyjną diagnostykę problemów. Wymagane są następujące funkcjonalności:

4.17.2. Funkcja diagnostyki błędów

4.17.2.1. System musi zapewniać pełną funkcjonalność diagnostyki błędów, obejmującą:

4.17.2.1.1. Zbieranie i analizę danych o błędach: Automatyczne gromadzenie danych diagnostycznych dotyczących kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde, zasilacze oraz wentylatory.

4.17.2.1.2. Diagnozowanie i lokalizowanie usterek: System musi umożliwiać automatyczne wykrywanie i lokalizowanie usterek sprzętowych, wskazując precyzyjnie wadliwe komponenty.

4.17.2.1.3. Wczesne ostrzeganie o błędach: Wymagane jest wsparcie dla funkcji wczesnego ostrzegania, które informuje użytkownika o potencjalnych problemach jeszcze przed ich wystąpieniem, co minimalizuje ryzyko awarii.

4.17.2.1.4. Analiza historii zdarzeń: System diagnostyczny musi umożliwiać przeglądanie pełnej historii zdarzeń oraz błędów, co ułatwia analizę przyczyn awarii i planowanie działań naprawczych.

4.17.3. Zaawansowane monitorowanie dysków twardych

4.17.3.1. System musi oferować szczegółowe monitorowanie stanu dysków twardych z podziałem na:

4.17.3.1.1. Alarmy dotyczące oprogramowania układowego dysku (firmware): Wykrywanie błędów związanych z oprogramowaniem układowym dysków oraz informowanie o konieczności aktualizacji firmware'u.

4.17.3.1.2. Alarmy dotyczące konfiguracji dysków: Monitorowanie nieprawidłowej konfiguracji dysków, takich jak problemy z RAID, oraz informowanie o konieczności interwencji.

4.17.3.1.3. Alarmy dotyczące usterek fizycznych: Wykrywanie błędów fizycznych dysków, takich jak problemy mechaniczne lub sektory uszkodzone, z możliwością precyzyjnego wskazania wadliwego dysku.

4.17.4. Monitoring temperatury i zarządzanie termiczne

4.17.4.1. System diagnostyczny musi zapewniać:

4.17.4.1.1. Graficzną mapę temperatury: Wymagana jest funkcjonalność przeglądania rozkładu temperatury wewnątrz serwera w formie graficznego modelu 3D. Mapa temperatury musi umożliwiać szybkie lokalizowanie anomalii termicznych.

4.17.4.1.2. Alerty dotyczące przekroczenia temperatur: Automatyczne powiadamianie o przekroczeniu dopuszczalnych wartości temperatury dla kluczowych komponentów, takich jak procesory, pamięć RAM czy zasilacze.

4.17.4.1.3. Dynamiczne zarządzanie chłodzeniem: System musi wspierać dynamiczne dostosowywanie prędkości wentylatorów na podstawie aktualnych odczytów temperatury, co zapewnia optymalną pracę serwera i minimalizuje zużycie energii.

4.17.5. Szyfrowane powiadomienia o błędach

4.17.5.1. Wymagane jest wsparcie dla szyfrowanych powiadomień o niekrytycznych i niekorygowalnych błędach (UCE), które umożliwiają precyzyjną identyfikację wadliwego modułu pamięci lub dysku.

4.17.5.2. System musi wspierać funkcję wysyłania powiadomień o błędach do administratora poprzez e-mail oraz protokoły zarządzania (np. SNMP, Redfish API).

4.17.6. Integracja z modułem zarządzania

4.17.6.1. System diagnostyczny musi być w pełni zintegrowany z modułem zarządzania iBMC, co umożliwia dostęp do danych diagnostycznych z poziomu interfejsu zarządzania.

4.17.6.2. Wymagana jest możliwość przeglądania szczegółowych raportów diagnostycznych oraz uruchamiania testów diagnostycznych w czasie rzeczywistym z poziomu konsoli zarządzającej.

4.18. Certyfikaty

4.18.1.1. Oferowany serwer musi być certyfikowany dla następujących środowisk:

- Microsoft Windows Server (wymagana zgodność z HCL Microsoft).
- Deklaracja CE dla oferowanego modelu serwera.
- Certyfikat EPEAT na poziomie min. Bronze

4.19. Parametry środowiskowe i efektywność energetyczna

4.19.1.1. Oferowane urządzenie musi udostępniać narzędzie, które zapewni możliwość bieżącej analizy poboru prądu.

4.19.1.2. Serwer musi być przystosowany do pracy w temperaturze od 5 do 45 stopni Celsjusza w sposób kompatybilny z wytycznymi ASHRAE A1 do A4.

4.19.1.3. Oferowane urządzenie musi być przystosowane do pracy w środowisku określonym normą ISO 14664-1.

4.20. Dokumentacja użytkownika

4.20.1.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera.

4.21. Warunki gwarancji

4.21.1.1. Zamawiający wymaga zapewnienia oficjalnego wsparcia Producenta w ramach oferowanej technologii na okres 3 lat w trybie NBD.

4.21.1.2. Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz maila.

4.21.1.3. Naprawa ma się odbywać się w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

4.21.1.4. Zamawiający dopuszcza aby wsparcie było świadczone przez autoryzowanego przedstawiciela serwisowego Producenta ale tylko jeżeli firma posiada certyfikację ISO 9001.

4.21.1.5. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

4.21.1.6. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.

4.22. System operacyjny serwera

4.22.1. Kompatybilność

4.22.1.1. Licencja systemu operacyjnego typu serwerowego – przeznaczonego do pracy w środowisku domenowym Zamawiającego, z zapewnieniem zgodności licencyjnej z posiadanymi przez Zamawiającego licencjami dostępowymi Client Access License (CAL) – User 2022 Windows Serwer 2022 Standard

4.22.1.2. system musi być w pełni zgodny z wdrożoną u Zamawiającego domeną Active Directory Domain Services pracującą w oparciu o system Windows Server 2022 Standard

4.22.2. Licencja

4.22.2.1. Licencja ma być udzielona na czas nieokreślony

4.22.2.2. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2

środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.

4.22.3. Wymagania funkcjonalno–techniczne:

4.22.3.1. możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek

4.22.3.2. możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu

4.22.3.3. system operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych łub o minimalnej wirtualizacji.

4.22.3.4. pełne wsparcie dla całej platformy .NET 4.0 oraz .NET 4.5

4.22.3.5. system operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6

4.22.3.6. system operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny

4.22.3.7. system operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.

4.22.3.8. system operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP

4.22.3.9. umożliwi uruchomienie serwera hostującego aplikacje ASP.NET

5. Zawansowane oprogramowanie do bezpieczeństwa XDR – 1szt.

5.1. LICENCJA

5.1.1.1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres do 30.06.2026 r..

5.1.1.2. Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. **12 miesięczną** gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).

5.1.1.3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.

5.1.1.4. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

5.1.1.5. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

5.1.1.6. Ilość licencji dla komputerów min.: **50 szt**.

5.1.1.7. Ilość licencji dla serwerów min.: **8 szt**.

5.2. Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych

5.2.1.1. System klasy EDR/XDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

5.2.1.2. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

5.2.1.3. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

5.2.1.4. Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

- Microsoft Windows 10
- Microsoft Windows 11
- MacOS 11 “Big Sur”
- MacOS 10.15 “Catalina”

- MacOS 10.14 “Mojave”
- MacOS 10.15 “Catalina”

5.2.1.5. Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2016
- Microsoft® Windows Server 2019
- Microsoft® Windows Server 2022

5.2.1.6. Wspierane przeglądarki internetowe:

5.2.1.6.1. • Microsoft Edge

5.2.1.6.2. • Mozilla Firefox

5.2.1.6.3. • Google Chrome

5.2.1.6.4. • Safari

5.2.1.7. Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

5.2.1.8. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.

5.2.1.9. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.

5.2.1.10. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.

5.2.1.11. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.

5.2.1.12. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.

5.2.1.13. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:

- dostęp do pliku;
- tworzenie nowego procesu;
- nawiązane połączenia sieciowe;
- wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
- zawartość skryptów uruchamianych na monitorowanej stacji.

5.2.1.14. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.

5.2.1.15. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.

5.2.1.16. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.

5.2.1.17. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).

5.2.1.18. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.

5.2.1.19. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.

5.2.1.20. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.

5.2.1.21. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.

5.2.1.22. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.

5.2.1.23. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.

5.2.1.24. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.

5.2.1.25. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.

5.2.1.26. Każda detekcja zawiera co najmniej następujące informacje:

- Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
- Data i czas wystąpienia podejrzanych zdarzeń.
- Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
- Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
- Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
- Poziom ryzyka, określający istotność danej detekcji.
- Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).

5.2.1.27. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).

5.2.1.28. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).

5.2.1.29. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.

5.2.1.30. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.

5.2.1.31. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.

5.2.1.32. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.

5.2.1.33. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.

5.2.1.34. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.

5.2.1.35. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.

5.2.1.36. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.

5.2.1.37. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.

5.2.1.38. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.

5.2.1.39. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.

5.2.1.40. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.

5.2.1.41. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.

5.2.1.42. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.

5.2.1.43. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.

5.2.1.44. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.

5.2.1.45. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.

5.2.1.46. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

5.2.1.47. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.

5.2.1.48. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

5.2.1.49. Opis technologii monitorowania podejrzanej aktywności na poziomie kont MS Entra ID

5.2.1.49.1. Rozwiązanie pozwala na synchronizację z usługami Entra ID

5.2.1.49.2. Rozwiązanie w przypadku wykrycia podejrzanie aktywności kont monitorowanych na poziomie Entra ID generuje detekcję widoczną w konsoli.

5.2.1.49.3. Wygenerowana detekcja posiada: ID Detekcji, określony poziom krytyczności, datę detekcji, datę ostatniej modyfikacji, status, informacje o dodanym komentarzu.

5.2.1.49.4. Administrator posiada możliwość wglądu w szczegóły danej detekcji.

5.2.1.49.5. W ramach szczegółów detekcji administrator ma możliwość manualnego określenia statusy detekcji, w zależności od etapu jej analizy.

5.2.1.49.6. Administrator posiada informacje dotyczące źródła detekcji, organizacji, dla której detekcja została wygenerowana, zasobu oraz lokacji dotkniętej wykrytą podejrzana aktywnością.

5.2.1.50. W ramach szczegółów detekcji administrator otrzymuje jej podsumowanie, opis, informacje o ryzyku z jakim związana jest dana aktywność oraz sugerowane rekomendacje.

5.2.1.51. Oprogramowanie do ochrony antymalware dla pakietu Microsoft 365, zapewniające zabezpieczenie usług poczty elektronicznej, przestrzeni współdzielonej oraz komunikacji zespołowej, integrujące się bezpośrednio z chmurowymi usługami producenta systemu bez konieczności instalacji dodatkowych serwerów w infrastrukturze użytkownika.

5.2.1.51.1. Rozwiązanie zapewnia ochronę antymalware dla pakietu Microsoft 365, obejmując ochronę poczty email MS Exchange, usługi MS SharePoint, usługi MS OneDrive oraz MS Teams.

5.2.1.51.2. Integruje się bezpośrednio z usługami Microsoft bez konieczności instalacji dodatkowych serwerów pośredniczących w środowisku klienta.

5.2.1.51.3. Zarządzanie odbywa się przez chmurową konsolę dostępną przez przeglądarkę internetową.

5.2.1.51.4. Konsola administracyjna umożliwia zarządzanie innymi produktami producenta, takimi jak endpoint protection, systemy EDR, mechanizmy zarządzania podatnościami – dostęp do funkcji zależny od typu licencji.

5.2.1.51.5. Wyposażone w dashboard podsumowujący stan ochrony i objętych ochroną usług.

5.2.1.51.6. Konfiguracja połączenia z usługami Microsoft odbywa się za pomocą kreatora.

5.2.1.51.7. Umożliwia określenie, czy ochroną objęte są wszystkie konta pocztowe czy tylko wybrane przez administratora.

5.2.1.51.8. Pozwala na tworzenie polityk konfiguracyjnych przypisywanych do poszczególnych usług.

5.2.1.51.9. Ochrona poczty Microsoft Exchange obejmuje mechanizmy ochrony antymalware w czasie rzeczywistym dla wiadomości przychodzących.

5.2.1.51.10. Obsługuje białe listy adresów email oraz domen.

5.2.1.51.11. Administrator może określić czas przechowywania obiektów w kwarantannie (1 miesiąc, 3 miesiące, 6 miesięcy, 1 rok).

5.2.1.51.12. Możliwość wyboru typów skanowanych plików oraz filtrowania po rozszerzeniach.

5.2.1.51.13. Obsługa skanowania wewnątrz plików archiwów.

5.2.1.51.14. Podejrzane pliki mogą być automatycznie detonowane w sandboxingu producenta.

5.2.1.51.15. W przypadku wykrycia zagrożenia możliwe działania: przeniesienie do kwarantanny, usunięcie wiadomości, usunięcie załącznika lub pozostawienie obiektu.

5.2.1.51.16. Obsługa powiadomień email o wykrytych zagrożeniach i personalizacja treści tych wiadomości.

5.2.1.51.17. Możliwość skanowania adresów URL pod kątem szkodliwej zawartości.

5.2.1.51.18. Wykrycie szkodliwego adresu URL pozwala na podjęcie działań: kwarantanna, usunięcie, zmiana tematu wiadomości, odlinkowanie.

5.2.1.51.19. Możliwość informowania administratora o wykrytych szkodliwych adresach URL.

5.2.1.51.20. Obsługa listy zaufanych i zablokowanych adresów URL.

5.2.1.51.21. Monitorowanie reguł poczty przychodzącej pod kątem podejrzanych działań (przenoszenie, usuwanie, przekazywanie emaili).

5.2.1.51.22. Monitorowanie chronionych kont email pod kątem wycieków danych oraz powiadamianie administratora.

5.2.1.51.23. W przypadku wycieku administrator uzyskuje szczegółowe informacje: adres email, źródło wycieku, forma wycieku hasła, data ostatniej zmiany hasła.

5.2.1.51.24. Mechanizm zarządzania kwarantanną umożliwiający administratorowi wgląd w szczegóły detekcji oraz możliwość usuwania i uwalniania obiektów z kwarantanny.

5.2.1.51.25. Możliwość generowania raportów dziennych, tygodniowych, miesięcznych w formacie PDF.

5.2.1.51.26. Skanowanie plików przesyłanych do objętej ochroną instancji MS SharePoint i MS OneDrive w ramach Microsoft 365.

5.2.1.51.27. Skanowanie wszystkich typów plików, plików o określonych rozszerzeniach oraz wykluczonych przez administratora.

5.2.1.51.28. Skanowanie plików archiwów i automatyczna detonacja podejrzanych obiektów w sandboxingu producenta.

5.2.1.51.29. W przypadku wykrycia zagrożenia na MS SharePoint i MS OneDrive możliwe podjęcie działań: kwarantanna, usunięcie lub brak akcji.

5.2.1.51.30. Możliwość skanowania obiektów dostępnych na platformie MS Teams w ramach organizacji.

5.2.1.51.31. Możliwość włączenia i wyłączenia automatycznego restartu w przypadku wymaganym przez instalację sterowników czy aplikacji.

5.2.1.51.32. Rozwiązanie monitoruje zmiany w konfiguracji ochrony i rejestruje je w logach audytowych.

5.2.1.51.33. Możliwość ręcznego przeskanowania obiektów na żądanie administratora.

5.2.1.51.34. Rozwiązanie może współpracować z dodatkowymi systemami klasy SIEM w celu lepszej analizy incydentów bezpieczeństwa.

5.2.1.51.35. Obsługa różnych poziomów uprawnień użytkowników w konsoli administracyjnej.

5.2.1.51.36. Możliwość definiowania harmonogramu skanowania dla różnych obszarów ochrony.

5.2.1.51.37. Automatyczne aktualizacje mechanizmów ochrony, baz sygnatur oraz silnika skanującego.

5.2.1.51.38. Obsługa powiadomień push dla administratorów w przypadku krytycznych zagrożeń.

5.2.1.51.39. Możliwość wdrożenia dodatkowych mechanizmów ochrony w zależności od poziomu licencji.

5.2.1.51.40. Możliwość integracji z narzędziami analityki zagrożeń producenta.

5.2.1.51.41. Pełne wsparcie dla środowisk hybrydowych Microsoft 365.

5.2.1.51.42. Możliwość eksportowania logów detekcji i działań administracyjnych do formatu XML.

5.2.1.51.43. Mechanizm wykrywania anomalii w ruchu sieciowym w kontekście przesyłania plików do chronionych zasobów.

5.2.1.51.44. Automatyczna synchronizacja polityk ochrony między różnymi usługami Microsoft 365.

5.2.1.51.45. Możliwość korzystania z zabezpieczeń wielopoziomowych, w tym dodatkowej autoryzacji administratora przy podejmowaniu krytycznych działań.

5.3. Certyfikaty i standardy

5.3.1.1. Oferowany produkt musi znajdować się w kwadracie Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms

5.3.1.1.1. minimalna ocena z referencji 4,5

5.3.1.2. Oferowany produkt musi znajdować się w kwadracie Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

5.3.1.2.1. minimalna ocena z referencji 4,4

5.3.2. System musi posiadać normy i certyfikaty:

5.3.2.1. OPSWAT (dla EDR/XDR na poziomie min. Platinium),

5.3.2.2. AV-TEST (ochrona w 2024 na poziomie min.6)

5.4. Rozszerzone wsparcie serwisowe

5.4.1.1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia **30.06.2026**.

5.4.1.2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Przygotowanie do zdalnej konfiguracji.
- Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

5.4.1.3. **Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.**

6. Zawansowane oprogramowanie do bezpieczeństwa AV – 1szt.

6.1. LICENCJA

6.1.1.1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres do 30.06.2026 .

6.1.1.2. Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. **12 miesięczną** gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).

6.1.1.3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.

6.1.1.4. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

6.1.1.5. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

6.1.1.6. Ilość licencji dla komputerów min.: **50 szt**.

6.1.1.7. Ilość licencji dla serwerów min.: **8 szt**.

6.2. Ochrona punktów końcowych urządzeń komputerowych

6.2.1.1. Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

6.2.1.2. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

6.2.1.3. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest

tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

6.2.1.4. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

- Microsoft Windows 10
- Microsoft Windows 11
- MacOS version 14 "Sonoma"
- MacOS version 13 "Ventura"
- MacOS version 12 "Monterey"

6.2.1.5. Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

6.2.1.6. Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

6.2.1.7. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

6.2.1.8. Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

6.2.1.9. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.

6.2.1.10. Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.

6.2.1.11. Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.

6.2.1.12. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych.

6.2.1.13. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.

6.2.1.14. Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:

- dostęp do pliku;
- tworzenie nowego procesu;
- nawiązane połączenia sieciowe;
- wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
- zawartość skryptów uruchamianych na monitorowanej stacji.

6.2.1.15. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.

6.2.1.16. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.

6.2.1.17. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.

6.2.1.18. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).

6.2.1.19. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.

6.2.1.20. Dane zbierane przez agentów na stacjach końcowych są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.

6.2.1.21. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.

6.2.1.22. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.

6.2.1.23. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym.

6.2.1.24. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.

6.2.1.25. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.

6.2.1.26. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.

6.2.1.27. Każda detekcja zawiera co najmniej następujące informacje:

- Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
- Data i czas wystąpienia podejrzanych zdarzeń.

- Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
- Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
- Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
- Poziom ryzyka, określający istotność danej detekcji.
- Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).

6.2.1.28. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).

6.2.1.29. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).

6.2.1.30. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.

6.2.1.31. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.

6.2.1.32. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.

6.2.1.33. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.

6.2.1.34. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.

6.2.1.35. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.

6.2.1.36. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.

6.2.1.37. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.

6.2.1.38. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.

6.2.1.39. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.

6.2.1.40. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.

6.2.1.41. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.

6.2.1.42. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.

6.2.1.43. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.

6.2.1.44. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.

6.2.1.45. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.

6.2.1.46. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.

6.2.1.47. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.

6.2.1.48. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)

6.2.1.49. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.

6.2.1.50. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.

6.2.1.51. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.

6.2.1.52. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.

6.2.1.53. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.

6.2.1.54. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.

6.2.1.55. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.

6.2.1.56. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.

6.2.1.57. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.

6.2.1.58. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja

automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.

6.2.1.59. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

6.2.1.60. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.

6.2.1.61. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.

6.2.1.62. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.

6.2.1.63. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.

6.2.1.64. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.

6.2.1.65. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

6.2.1.66. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.

6.2.1.67. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.

6.2.1.68. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.

6.2.1.69. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.

6.2.1.70. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.

6.2.1.71. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.

6.2.1.72. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym

6.2.1.73. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

6.2.1.74. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

6.2.1.75. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.

6.2.1.76. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".

6.2.1.77. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.

6.2.1.78. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.

6.2.1.79. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.

6.2.1.80. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.

6.2.1.81. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.

6.2.1.82. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.

6.2.1.83. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.

6.2.1.84. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.

6.2.1.85. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

6.2.1.86. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.

6.2.1.87. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.

6.2.1.88. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.

6.2.1.89. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.

6.2.1.90. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.

6.2.1.91. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.

6.2.1.92. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.

6.2.1.93. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.

6.2.1.94. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.

6.2.1.95. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

6.2.1.96. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna".

6.2.1.97. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna" rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.

6.2.1.98. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna" rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.

6.2.1.99. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.

6.2.1.100. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna" czyści zawartość schowka systemowego.

6.2.1.101. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.

6.2.1.102. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

6.2.1.103. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.

6.2.1.104. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).

6.2.1.105. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.

6.2.1.106. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.

6.2.1.107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.

6.2.1.108. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.

6.2.1.109. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.

6.2.1.110. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.

6.2.1.111. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.

6.2.1.112. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.

6.2.1.113. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.

6.2.1.114. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.

6.2.1.115. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.

6.2.1.116. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.

6.2.1.117. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.

6.2.1.118. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.

6.2.1.119. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.

6.2.1.120. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.

6.2.1.121. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.

6.2.1.122. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.

6.2.1.123. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.

6.2.1.124. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.

6.2.1.125. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.

6.2.1.126. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.

6.2.1.127. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker

6.2.1.128. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.

6.2.1.129. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.

6.2.1.130. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.

6.2.1.131. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.

6.2.1.132. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.

6.2.1.133. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)

6.2.1.134. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.

6.2.1.135. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.

6.2.1.136. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.

6.2.1.137. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.

6.2.1.138. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu

polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

6.2.1.139. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.

6.2.1.140. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

6.2.1.141. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

6.2.1.142. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.

6.2.1.143. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.

6.2.1.144. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.

6.2.1.145. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.

6.2.1.146. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.

6.2.1.147. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.

6.2.1.148. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.

6.2.1.149. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN

6.2.1.150. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)

6.2.1.151. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.

6.2.1.152. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).

6.2.1.153. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

6.2.2. Centralna administracja

6.2.2.1. Portal zarządzający jest dostępny w języku polskim.

6.2.2.2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.

6.2.2.3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.

6.2.2.4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.

6.2.2.5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.

6.2.2.6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.

6.2.2.7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane

oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.

6.2.2.8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.

6.2.2.9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.

6.2.2.10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.

6.2.2.11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.

6.2.2.12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.

6.2.2.13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.

6.2.2.14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.

6.2.2.15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.

6.2.2.16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.

6.2.2.17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.

6.2.2.18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.

6.2.2.19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.

6.2.2.20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

6.2.2.21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.

6.2.2.22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

6.2.2.23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.

6.2.2.24. Profile mogą być przypisane do pojedynczych hostów lub do grup.

6.2.2.25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.

6.2.2.26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.

6.2.2.27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.

6.2.2.28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.

6.2.2.29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.

6.2.2.30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.

6.2.2.31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.

6.2.2.32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.

6.2.2.33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.

6.2.2.34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.

6.2.2.35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.

6.2.2.36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji

6.3. Certyfikaty i standardy

6.3.1.1. Oferowany produkt musi znajdować się w kwadracie Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms

6.3.1.1.1. minimalna ocena z referencji 4,5

6.3.1.2. Oferowany produkt musi znajdować się w kwadracie Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

6.3.1.2.1. minimalna ocena z referencji 4,4

6.3.2. System musi posiadać certyfikaty:

6.3.2.1. OPSWAT (dla EDR na poziomie min. Platinium),

6.3.2.2. AV Comperative Advance +

6.3.2.3. AV-TEST (ochrona w 2024 na poziomie min.6)

6.4. Rozszerzone wsparcie serwisowe

6.4.1.1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia **30.06.2026**.

6.4.1.2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

6.4.1.2.1. • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.

6.4.1.2.2. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.

6.4.1.2.3. • Doradztwo w zakresie konfiguracji.

6.4.1.2.4. • Zdalne wsparcie techniczne.

6.4.1.2.5. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.

6.4.1.2.6. • Przygotowanie do zdalnej konfiguracji.

6.4.1.2.7. • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.

6.4.1.2.8. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.

6.4.1.2.9. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.

6.4.1.2.10. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

6.4.1.3. **Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.**

7. System NAC

7.1. Podstawowa funkcjonalność systemu NAC:

7.1.1.1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.

7.1.1.2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)

7.1.1.3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.

7.1.1.4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.

7.1.1.5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.

7.1.1.6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.

7.1.1.7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.

7.1.1.8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.

7.1.1.9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.

7.1.1.10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:

- VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
- Maszyny fizyczne - serwery wspierane przez producenta.

7.1.1.11. System musi posiadać funkcjonalność serwerów:

- serwera RADIUS dla infrastruktury sieciowej,
- serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
- serwera SYSLOG,
- serwera TACACS+,
- serwera Monitoringu,
- serwera DHCP,
- serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
- serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.

7.1.1.12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.

7.1.1.13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.

7.1.1.14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.

7.1.1.15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP,

relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.

7.1.1.16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.

7.1.1.17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.

7.1.1.18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.

7.1.1.19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.

7.1.1.20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.

7.1.1.21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).

7.1.1.22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.

7.1.1.23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).

7.1.1.24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.

7.1.1.25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.

7.1.1.26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.

7.1.1.27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.

7.1.1.28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.

7.1.1.29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.

7.1.1.30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.

7.1.1.31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.

7.1.1.32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.

7.1.1.33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

7.1.1.34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.

7.1.1.35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.

7.1.1.36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).

7.1.1.37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.

7.1.1.38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.

7.1.1.39. System musi posiadać funkcję personalizacji strony gościnnej.

7.1.1.40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.

7.1.1.41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.

7.1.1.42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.

7.1.1.43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.

7.1.1.44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.

7.1.1.45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.

7.1.1.46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.

7.1.1.47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).

7.1.1.48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.

7.1.1.49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.

7.1.1.50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.

7.1.1.51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.

7.1.1.52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.

7.1.1.53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.

7.1.1.54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.

7.1.1.55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.

7.1.1.56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.

7.1.1.57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).

7.1.1.58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.

7.1.1.59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:

- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
- Czy włączony jest firewall
- Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
- Czy jest włączone szyfrowanie dysku systemowego
- Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
- Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
- Czy w systemie są uruchomione procesy wskazane przez administratora
- Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
- Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:

- Wartości klucza rejestru
- Typu wartości: Number, String, Version

7.1.1.60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

7.1.1.61. System musi współpracować z serwerem tokenów.

7.1.1.62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:

- Microsoft Windows
- Mac OS
- iOS
- Android

7.1.1.63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).

7.1.1.64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

7.2. Mechanizmy uwierzytelniania

7.2.1.1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

7.2.1.2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

- MAC,
- PAP/ASCII,
- CHAP,
- SNMP,
- 802.1X.

7.2.1.3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.

7.2.1.4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

7.2.1.5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.

7.2.1.6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).

7.2.1.7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

- Tożsamość/Urządzenie końcowe,
- Grupa tożsamości/urządzeń końcowych,
- Parametry urządzeń końcowych, min: system operacyjny, wersja,
- Atrybuty Active Directory,
- Jednostka organizacyjna tożsamości/urządzeń końcowych,
- Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
- Grupy urządzeń sieciowych,
- Porty urządzeń sieciowych,
- Grupy portów urządzeń sieciowych,
- Jednostka organizacyjna portów,
- Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
- Data, czas ważności polityki,
- Wewnętrzny Captive Portal,
- Metoda autoryzacji.

7.2.1.8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard

Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.

7.2.1.9. System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

7.2.1.10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.

7.2.1.11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.

7.2.1.12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.

7.2.1.13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.

7.2.1.14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.

7.2.1.15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.

7.2.1.16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.

7.2.1.17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.

7.2.1.18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.

7.2.1.19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.

7.2.1.20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

7.3. Obsługa serwerów certyfikatów CA

7.3.1.1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.

7.3.1.2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:

- możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
- możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
- Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
- usługę OCSP (Online Certificate Status Protocol).

7.4. Obsługa serwerów DHCP

7.4.1.1. System musi posiadać funkcję zintegrowanego serwera DHCP.

7.4.1.2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.

7.4.1.3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:

- Uruchamianie usługi dla wybranych podsieci,
- Przypisanie ustalonego adresu IP dla adresu MAC.
- Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
- Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
- Możliwość określania braku dostępu dla wybranych adresów MAC,

- Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
- Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
- Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączania usług.

7.5. Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

7.5.1.1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.

7.5.1.2. System musi umożliwiać tworzenia haseł administratorom.

7.5.1.3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów

7.5.1.4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.

7.5.1.5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.

7.5.1.6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.

7.5.1.7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.

7.5.1.8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

7.6. Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

7.6.1.1. Monitoring autoryzacji.

7.6.1.2. Monitoring dla zdarzeń systemowych.

7.6.1.3. Monitoring dla zdarzeń DHCP.

7.6.1.4. Monitoring dla tożsamości.

7.6.1.5. Monitoring dla urządzeń końcowych.

7.6.1.6. Monitoring dla urządzeń sieciowych.

7.6.1.7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.

7.6.1.8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.

7.6.1.9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.

7.6.1.10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.

7.6.1.11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.

7.6.1.12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.

7.6.1.13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.

7.6.1.14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.

7.6.1.15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.

7.6.1.16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.

7.6.1.17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.

7.6.1.18. Raport zdarzeń Microsoft Active Directory, minimum:

- Logowania, wylogowania z system w tym błędne logowania
- Logowania do sieci 802.1X

7.7. Alarmy

7.7.1.1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:

- wiadomości e-mail,
- Syslog,
- notyfikacji systemowych.

7.7.1.2. Alarmy mogą być generowane w sytuacjach, min:

- Ilości obsługiwanych transakcji RADIUS,
- Opóźnienie obsługi transkacji RADIUS,
- Statusu krytycznego modułów.

7.7.1.3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

- badanie łączności IP za pomocą ping, traceroute,
- tcpdump protokołów RADIUS, TACACS+,
- wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
  - nazwy użytkownika,
  - adresu MAC,
  - statusu uwierzytelnienia (udana lub nieudana),
  - powodu, jeżeli uwierzytelnienie nieudane,
  - zakresu czasowego, co do dnia, godziny i minuty,
- wykonanie zdalnego polecenia na urządzeniu sieciowym.

7.8. Wymagania dotyczące wdrożenia i harmonogram ramowy:

7.8.1.1. Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.

7.8.1.2. Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).

7.8.1.3. Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).

7.8.1.4. Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).

7.8.1.5. Integracja dostarczanych urządzeń sieciowych wzorcowych po jednym z każdej serii (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.

7.8.1.6. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.

7.8.1.7. Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.

7.8.1.8. Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

7.9. Licencja wsparcia technicznego producenta oprogramowania:

7.9.1.1. Wykonawca dostarczy wraz dożywotnią licencją systemu NAC -do 30.06.2026r. licencje na wsparcie producenta oprogramowania.

7.9.1.2. Licencja wsparcia powinna obejmować minimum:

7.9.1.2.1. • Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC

7.9.1.2.2. • Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.

7.9.1.2.3. • Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.

7.9.1.2.4. • Dostęp do dokumentacji i instrukcji na stronie internetowej.

7.9.1.2.5. • Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

8. Przełącznik sieciowy 48 portowy gigabitowy – 4 sztuki.

8.1. Minimalne parametry techniczne

8.1.1.1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T ze wsparciem dla trybów: full-duplex, half-duplex, automatycznej negocjacji (auto-negotiation)

8.1.1.2. Minimum 4 porty 1/10Gb SFP/SFP+, pozwalające na instalację wkładek 10Gb (SFP+), Gigabitowych (SFP) oraz kabli DAC/Twinax SFP+

8.1.1.3. Minimum 2 porty 10GE lub szybsze umożliwiające budowę stosu przełączników.

8.1.1.4. Automatyczne wykrywanie przeplotu (Auto MDIX) na portach 10/100/1000Base-T

8.1.1.5. Przepustowość: minimum 224 Gbps oraz minimum 160 Mpps.

8.1.1.6. Tablica adresów MAC o wielkości minimum 32 000 pozycji

8.1.1.7. Obsługa ramek Jumbo: minimum 9kb

8.1.1.8. Przełącznik wyposażony w co najmniej jeden zasilacz 230V/AC.

8.1.1.9. Urządzenie musi mieć możliwość łączenia przełączników fizycznych w jeden

8.1.1.10. przełącznik wirtualny (tzw. Stos), traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree.

8.1.1.11. Minimalna liczba przełączników obsługiwanych w stosie: 9szt

8.1.1.12. Funkcja tworzenia stosu nie może wykorzystywać czterech portów Uplink 10GE SFP+

8.1.1.13. Prędkość magistrali tworzącej stos: minimum 80 Gbps (Bidirectional)

8.1.1.14. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)

8.1.1.15. Obsługa standardu LACP (Link Aggregation Control Protocol) z obsługą minimum 24 grup po 8 portów w grupie (w obrębie stosu przełączników)

8.1.1.16. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie

8.1.1.17. Tablica ARP minimum 2000 wpisów

8.1.1.18. Tablica routingu nie mniejsza niż 4000 wpisów dla IPv4 i 1000 wpisów dla IPv6

8.1.1.19. Minimum 1000 interfejsów VLAN

8.1.1.20. Routing IPv4 – minimum: statyczny (minimum 4000 tras), RIPv1, RIPv2, OSPF

8.1.1.21. Routing IPv6 – minimum: statyczny (minimum 1000 tras), RIPng, OSPFv3

8.1.1.22. Obsługa VRRP i VRRP6

8.1.1.23. Obsługa ruchu Multicast: PIM-DM, PIM-SM, PIM-DM dla IPv6, IGMP v1/v2/v3, IGMP v1/v2/v3 Snooping;

8.1.1.24. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol

8.1.1.25. Obsługa protokołu PVST lub równoważnego.

8.1.1.26. Wsparcie dla protokołu typu Ethernet Ring Protection Switching (ERPS, G.8032)

8.1.1.27. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 aktywnych sieci VLAN

8.1.1.28. Obsługa IEEE 802.1ad QinQ

8.1.1.29. Funkcja Root Protection umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree

8.1.1.30. Funkcja BPDU Protection – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom

8.1.1.31. Wsparcie dla funcji DHCP Relay, DHCP client oraz DHCP Snooping

8.1.1.32. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI

8.1.1.33. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)

8.1.1.34. Obsługa standardu 802.1p – min. 8 kolejek na porcie

8.1.1.35. Funkcja wyboru sposobu obsługi kolejek, minimum – Strict Priority (SP); Weighted Round Robin (WRR) lub równoważny; WRR + SP lub równoważne.

8.1.1.36. Funkcja mirroringu portów: SPAN

8.1.1.37. Obsługa funkcji logowania do sieci zgodna ze standardem IEEE 802.1x oraz autoryzacja po adresach MAC. Obsługa serwerów TACACS+ i RADIUS

8.1.1.38. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED

8.1.1.39. Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS

8.1.1.40. Obsługa funkcji Voice VLAN

8.1.1.41. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, https

8.1.1.42. Port konsoli RS232 ze złączem RJ45

8.1.1.43. Port USB 2.0

8.1.1.44. Obsługa Syslog

8.1.1.45. Obsługa NTP (Network Time Protocol)

8.1.1.46. Obsługa RMON (minimum grupy 1/2/3/9)

8.1.1.47. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania)

8.1.1.48. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

8.1.1.49. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

8.1.1.50. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego

8.1.1.51. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych

8.1.1.52. Minimalny zakres pracy od 0°C do +50°C

8.1.1.53. Wysokość w szafie 19” – 1U

8.1.1.54. Maksymalny pobór mocy nie większy niż 100 W

8.1.1.55. Ochrona przepięciowa, nie gorsza niż 1.5kV dla portów przełącznika oraz zasilaczy AC.

8.2. Warunki gwarancyjne

8.2.1.1. Zamawiający wymaga, aby przełączniki posiadały min. 3-letnią gwarancję świadczoną przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie NBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.

8.2.1.2. Zamawiający dopuszcza aby wsparcie było świadczone przez autoryzowanego przedstawiciela serwisowego Producenta ale tylko jeżeli firma posiada certyfikację ISO 9001.

9. UTM

9.1. Kompatybilność

9.1.1.1. Dostawa, instalacja i konfiguracja urządzenia klasy **UTM (Unified Threat Management,** zapewniającego pełną funkcjonalną i zarządczą kompatybilność z posiadanym przez Zamawiającego systemem zabezpieczeń opartym na urządzeniu **Stormshield**

SN310. Urządzenie musi być **w pełni kompatybilne z oprogramowaniem zarządzającym** i konfiguracją istniejącego rozwiązania **Stormshield SN310**, w tym w szczególności:

9.1.1.1.1. możliwość eksportu/importu polityk bezpieczeństwa pomiędzy SN310 a nowym urządzeniem,

9.1.1.1.2. spójność logów i raportów

9.1.1.1.3. możliwość zestawienia połączenia HA (High Availability) z urządzeniem SN310.

9.1.1.1.4. możliwości tworzenia połączeń IPSEC VPN przy użyciu interfejsu VTI (Virtual Tunneling Interface) z SN310

9.2. Wymagania funkcjonalno–techniczne:

9.2.1. Urządzenie UTM musi realizować zintegrowane funkcje bezpieczeństwa sieciowego, w tym co najmniej:

9.2.1.1. zaporę ogniową (firewall) z kontrolą aplikacji,

9.2.1.2. system wykrywania i zapobiegania włamaniom (IPS/IDS),

9.2.1.3. filtrowanie treści WWW (URL filtering),

9.2.1.4. ochronę antywirusową i antymalware,

9.2.1.5. ochronę przed spamem,

9.2.1.6. VPN (IPSec oraz SSL),

9.2.1.7. kontrolę przepływu ruchu (QoS).

9.2.1.8. wsparcie IPv4/IPv6, VLAN, dynamiczne routowanie, SNMP.

9.2.1.9. Zarządzanie łączami WAN i SD-WAN

9.2.2. Parametry techniczne

9.2.2.1. przepustowość zapory (1518-bajtowa ramka danych) min. 8 Gbps

9.2.2.2. przepustowość IPS (1518-bajtowa ramka danych) min. 4 Gbps,

9.2.2.3. Przepustowość IPSEC VPN min. 2 Gbps

9.2.2.4. Przepustowość Antywirusa min. 1 Gbps

9.2.2.5. co najmniej 8 portów Ethernet 100/1000/2500

9.2.2.6. Liczba jednoczesnych połączeń klientów SSL VPN: 100

9.2.2.7. Pamięć lokalna Karta MicroSD

9.2.2.8. Układ TPM

9.1. Licencja wsparcia technicznego producenta oprogramowania

9.1.1.1. Wykonawca dostarczy urządzenie z ważną licencją subskrypcyjną na okres do 30.06.2026. Pakiet wsparcia UTM (IPS, zaawansowany AV, filtracja URL min. 65 kategorii, Antyspam, aktualizacje firmware)

9.2. Warunki gwarancyjne

9.2.1.1. Gwarancja producenta lub autoryzowanego partnera producenta na okres min. 12 miesięcy,

9.2.1.2. Wsparcie techniczne w języku polskim

10. Szkolenie stacjonarne dla pracowników Urzędu z zakresu cyberbezpieczeństwa

10.1.1. Cele szkolenia

10.1.1.1. Podniesienie świadomości pracowników Urzędu w zakresie cyberbezpieczeństwa.

10.1.1.2. Zapoznanie uczestników z podstawowymi pojęciami i zagadnieniami dotyczącymi cyberzagrożeń.

10.1.1.3. Przekazanie zasad bezpiecznego korzystania z systemów informatycznych i sieci.

10.1.1.4. Przygotowanie pracowników do prawidłowego reagowania na incydenty bezpieczeństwa.

10.1.2. Zasady realizacji szkoleń

10.1.2.1. Szkolenie realizowane będzie w formie stacjonarnej w siedzibie Zamawiającego.

10.1.2.2. Uczestnicy zostaną podzieleni na 2 grupy w celu zapewnienia efektywnej realizacji zajęć.

10.1.2.3. Liczba uczestników w grupie nie przekroczy 20 osób.

10.1.2.4. Dla każdej grupy przewidziane zostanie szkolenie o wymiarze co najmniej 2 godzin dydaktycznych.

10.1.2.5. Zamawiający dopuszcza rotację liczby uczestników podczas każdego cyklu szkoleniowego.

10.1.2.6. Szkolenia odbywać się będą w dni robocze (poniedziałek–piątek) w godzinach 8:00–15:00.

10.1.2.7. Wykonawca zapewni materiały szkoleniowe w wersji papierowej dla wszystkich uczestników.

10.1.2.8. Każdy uczestnik otrzyma **certyfikat ukończenia szkolenia**.

10.1.3. Zakres merytoryczny szkolenia (minimum)

10.1.3.1. Wprowadzenie do cyberbezpieczeństwa:

- definicja i znaczenie cyberbezpieczeństwa,
- kluczowe pojęcia i terminologia,
- przegląd statystyk i trendów.

10.1.3.2. Typy zagrożeń w cyberprzestrzeni

- malware (wirusy, trojany, robaki),
- phishing i spear phishing,
- ataki DDoS,
- ransomware,
- zagrożenia związane z mediami społecznościowymi

10.1.3.3. Zasady bezpieczeństwa i praktyki

- zarządzanie hasłami i MFA,
- bezpieczeństwo poczty elektronicznej,
- bezpieczne korzystanie z sieci Wi-Fi,
- bezpieczne przeglądanie stron WWW,
- backup i odzyskiwanie danych.

10.1.3.4. Reagowanie na incydenty i planowanie awaryjne

- identyfikacja i zgłaszanie incydentów,
- podstawowe procedury reagowania,
- planowanie awaryjne i ciągłość działania,

- analiza realnych przypadków naruszeń.

10.1.4. Dokumentacja szkolenia

10.1.4.1. W ramach realizacji usługi Wykonawca zobowiązany jest do przekazania

10.1.4.1.1. list obecności uczestników,

10.1.4.1.2. list odbioru certyfikatów,

10.1.4.1.3. dzienników szkoleń (zakres tematyczny + podpis prowadzącego),

11. Szkolenia dla administratorów z nowych technologii

11.1. Szkolenie z SIEM

11.1.1. Cele szkolenia

11.1.1.1. Przygotowanie administratora i do efektywnego korzystania z systemów SIEM w zakresie monitorowania, analizy i reagowania na incydenty bezpieczeństwa.

11.1.1.2. Nabycie praktycznych umiejętności konfiguracji, integracji i zarządzania regułami w SIEM.

11.1.1.3. Podniesienie kompetencji w obszarze analizy logów, korelacji zdarzeń oraz raportowania.

11.1.1.4. Zwiększenie zdolności organizacji do szybkiego wykrywania i reagowania na cyberzagrożenia.

11.1.2. Zakres tematyczny

11.1.2.1. Wprowadzenie do SIEM

- Rola i znaczenie SIEM w systemie bezpieczeństwa organizacji.
- Architektura systemów SIEM.
- Przegląd wiodących rozwiązań dostępnych na rynku.

11.1.2.2. Gromadzenie i przetwarzanie logów

- Źródła logów (serwery, systemy operacyjne, urządzenia sieciowe, aplikacje).

- Normalizacja danych i parsowanie logów.
- Tworzenie i zarządzanie konektorami.

11.1.2.3. Korelacja zdarzeń i reguły detekcji

- Podstawowe i zaawansowane mechanizmy korelacji.
- Tworzenie i optymalizacja reguł wykrywania.
- Minimalizacja liczby false positives.

11.1.2.4. Analiza zdarzeń i reagowanie na incydenty

- Analiza w czasie rzeczywistym i analiza retrospektywna.
- Procedury reagowania na alerty i incydenty.
- Integracja SIEM z SOC, SOAR i EDR.

11.1.2.5. Raportowanie i compliance

- Tworzenie raportów technicznych i menedżerskich.
- Raporty zgodności (RODO, KSC, ISO 27001).
- Wizualizacja danych w dashboardach SIEM.

11.1.2.6. Praktyczne ćwiczenia

- Konfiguracja systemu SIEM i dodawanie źródeł logów.
- Tworzenie reguł korelacyjnych i scenariuszy detekcji.
- Analiza przykładowych incydentów i przygotowanie raportów.

11.1.3. Forma realizacji

11.1.3.1. **Czas trwania:** 12 godzin (6 godzin teorii + 6 godzin praktyki).

11.1.3.2. **Forma:** Szkolenie stacjonarne lub zdalne.

11.1.3.3. **Materiały**: Dokumentacja użytkownika, scenariusze ataków i ćwiczeń, przykładowe logi do analizy (w wersji papierowej i/lub elektronicznej).

11.1.3.4. **Certyfikat:** Uczestnik otrzyma certyfikat ukończenia szkolenia.

11.1.4. Dokumentacja szkolenia

11.1.4.1. W ramach realizacji usługi Wykonawca zobowiązany jest do przekazania

11.1.4.1.1. list obecności uczestników,

11.1.4.1.2. list odbioru certyfikatów,

11.1.4.1.3. dzienników szkoleń (zakres tematyczny + podpis prowadzącego)

11.2. Szkolenie z EDR (Endpoint Detection and Response)

11.2.1. Cele szkolenia

11.2.1.1. Przygotowanie administratora do skutecznej ochrony stacji roboczych i serwerów przed zaawansowanymi zagrożeniami.

11.2.1.2. Nabycie umiejętności w zakresie wdrażania, monitorowania i reagowania na incydenty bezpieczeństwa.

11.2.1.3. Zrozumienie architektury systemów EDR i ich integracji z innymi rozwiązaniami bezpieczeństwa.

11.2.2. Zakres tematyczny

11.2.2.1. Wprowadzenie do EDR

11.2.2.1.1. Podstawowe funkcje i zastosowania EDR.

11.2.2.1.2. Różnice między EDR a tradycyjnymi rozwiązaniami antywirusowymi.

11.2.2.1.3. Przegląd wiodących technologii i dostawców.

11.2.2.2. Konfiguracja i zarządzanie politykami

11.2.2.2.1. Tworzenie reguł wykrywania i blokowania.

11.2.2.2.2. Definiowanie polityk dla różnych grup użytkowników i zasobów.

11.2.2.3. Monitorowanie i analiza zdarzeń

11.2.2.3.1. Przegląd konsoli i dashboardów analitycznych.

11.2.2.3.2. Analiza logów i alertów w czasie rzeczywistym.

11.2.2.4. Reagowanie na incydenty

11.2.2.4.1. Procedury izolowania i neutralizacji zagrożeń.

11.2.2.4.2. Tworzenie raportów powłamaniowych.

11.2.2.4.3. Współpraca z zespołem SOC lub CSIRT.

11.2.2.5. Zaawansowane funkcje EDR:

11.2.2.5.1. Threat hunting – wyszukiwanie ukrytych zagrożeń.

11.2.2.5.2. Integracja z SIEM, SOAR i systemami AV/NGAV.

11.2.3. Forma realizacji

11.2.3.1. **Czas trwania:** 12 godzin (6 godzin teorii + 6 godzin praktyki).

11.2.3.2. **Forma:** Szkolenie stacjonarne lub zdalne (warsztaty z ćwiczeniami).

11.2.3.3. **Materiały:** Przewodniki użytkownika, scenariusze ataków i ćwiczeń, przykładowe logi do analizy (w wersji papierowej i/lub elektronicznej).

11.2.4. Dokumentacja szkolenia

11.2.4.1. W ramach realizacji usługi Wykonawca zobowiązany jest do przekazania

11.2.4.1.1. list obecności uczestników,

11.2.4.1.2. list odbioru certyfikatów,

11.2.4.1.3. dzienników szkoleń (zakres tematyczny + podpis prowadzącego)

11.3. Szkolenie ze skanera podatności

11.3.1. Cele szkolenia

11.3.1.1. Przygotowanie administratora do skutecznego wykrywania i zarządzania podatnościami w infrastrukturze IT.
Nabycie umiejętności konfiguracji, uruchamiania i interpretacji wyników skanów.
Zrozumienie procesu zarządzania ryzykiem oraz priorytetyzacji działań naprawczych.

11.3.2. Zakres tematyczny

11.3.2.1. Wprowadzenie do skanowania podatności:

- Cele i znaczenie skanowania podatności.
- Typy podatności (systemowe, aplikacyjne, sieciowe).
- Przegląd narzędzi i technologii (komercyjnych i open-source).

11.3.2.2. Instalacja i konfiguracja skanera:

- Wymagania środowiskowe i sieciowe.
- Tworzenie polityk skanowania.

- Harmonogramy i automatyzacja.

11.3.2.3. Wykonywanie skanów:

- Skanowanie urządzeń sieciowych i systemów operacyjnych.
- Analiza aplikacji webowych.
- Testowanie konfiguracji i zgodności (compliance).

11.3.2.4. Analiza i raportowanie wyników:

- Interpretacja wyników i priorytetyzacja podatności.
- Tworzenie raportów technicznych i menedżerskich.
- Integracja wyników z systemami ticketowymi i SIEM.

11.3.2.5. Zarządzanie ryzykiem i remediacja:

- Dobór działań naprawczych i proces patch management.
- Weryfikacja poprawy po wdrożeniu łatek.
- Tworzenie planu cyklicznych skanów.

11.3.3. Forma realizacji

11.3.3.1. **Czas trwania:** 10 godzin (4 godziny teorii + 6 godzin praktyki).

11.3.3.2. **Forma:** Stacjonarne lub zdalne warsztaty praktyczne.

11.3.3.3. **Materiały:** Instrukcje konfiguracji, przykładowe raporty (w wersji papierowej i/lub elektronicznej),

11.3.4. Dokumentacja szkolenia

11.3.4.1. W ramach realizacji usługi Wykonawca zobowiązany jest do przekazania

11.3.4.1.1. list obecności uczestników,

11.3.4.1.2. list odbioru certyfikatów,

11.3.4.1.3. dzienników szkoleń (zakres tematyczny + podpis prowadzącego),

11.4. Szkolenie z Systemu kontroli dostępu do sieci (NAC)

11.4.1. Cele szkolenia:

11.4.1.1. Wyposażenie administratora w wiedzę i umiejętności niezbędne do skutecznego zarządzania dostępem użytkowników do sieci.

11.4.1.2. Wdrażanie polityk bezpieczeństwa zgodnie z zasadą minimalnego dostępu.

11.4.2. Zakres tematyczny:

11.4.2.1. Podstawy NAC:

- Omówienie funkcji i korzyści.
- Architektura systemu kontroli dostępu.

11.4.2.2. Konfiguracja polityk dostępu:

- Tworzenie reguł kontroli urządzeń i użytkowników.
- Definiowanie poziomów dostępu do zasobów sieciowych.

11.4.2.3. Integracja z infrastrukturą:

- Powiązanie NAC z istniejącymi rozwiązaniami (np. Active Directory).
- Zarządzanie urządzeniami w sieci.

11.4.2.4. Monitorowanie i analiza:

- Śledzenie aktywności użytkowników.
- Generowanie raportów zgodności.

11.4.2.5. Reagowanie na naruszenia:

- Automatyczne izolowanie zagrożeń.
- Procedury eskalacji i rozwiązywania incydentów.

11.4.3. Forma realizacji:

11.4.3.1. **Czas trwania:** 14 godzin (7 godzin teoretycznych + 7 godzin warsztatowych).

11.4.3.2. **Forma:** Stacjonarne lub zdalne warsztaty z ćwiczeniami praktycznymi.

11.4.3.3. **Materiały:** Dokumentacja techniczna oraz przykładowe scenariusze wdrożeniowe (w wersji papierowej i/lub elektronicznej).

11.4.4. Dokumentacja szkolenia

W ramach realizacji usługi Wykonawca zobowiązany jest do przekazania

11.4.4.1.1. list obecności uczestników,

11.4.4.1.2. list odbioru certyfikatów,

11.4.4.1.3. dzienników szkoleń (zakres tematyczny + podpis prowadzącego)