

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

Na potrzeby przetargu otwartego na dostawę pn. „Rozwój cyberbezpieczeństwa w PWiK Żory Sp. z o.o.”, realizowanego w ramach projektu „Cyberbezpieczne Wodociągi”, Inwestycja C3.1.1 „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo”, ujętej w Krajowym Planie Odbudowy i Zwiększania Odporności, finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

Wymagania ogólne

Przedmiotem zamówienia jest dostawa sprzętu IT, wraz z oprogramowaniem, udzieleniem licencji na oprogramowania i sprzęt oraz wdrożenie systemów cyberbezpieczeństwa, rozumiane jako instalacja, testy, konfiguracja, a także przeprowadzenie szkoleń w zakresie obsługi wdrożonych urządzeń i systemów oraz przeprowadzenie audytów w ramach Projektu grantowego dla przedsięwzięcia pod nazwą „Rozwój cyberbezpieczeństwa w PWiK Żory Sp. z o.o.” realizowanego w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczne Wodociągi. Konkurs grantowy pn. „Cyberbezpieczne Wodociągi” o numerze KPOD.05.10-CW.01-001/25. Przedmiot zamówienia został podzielony na dwa zadania :

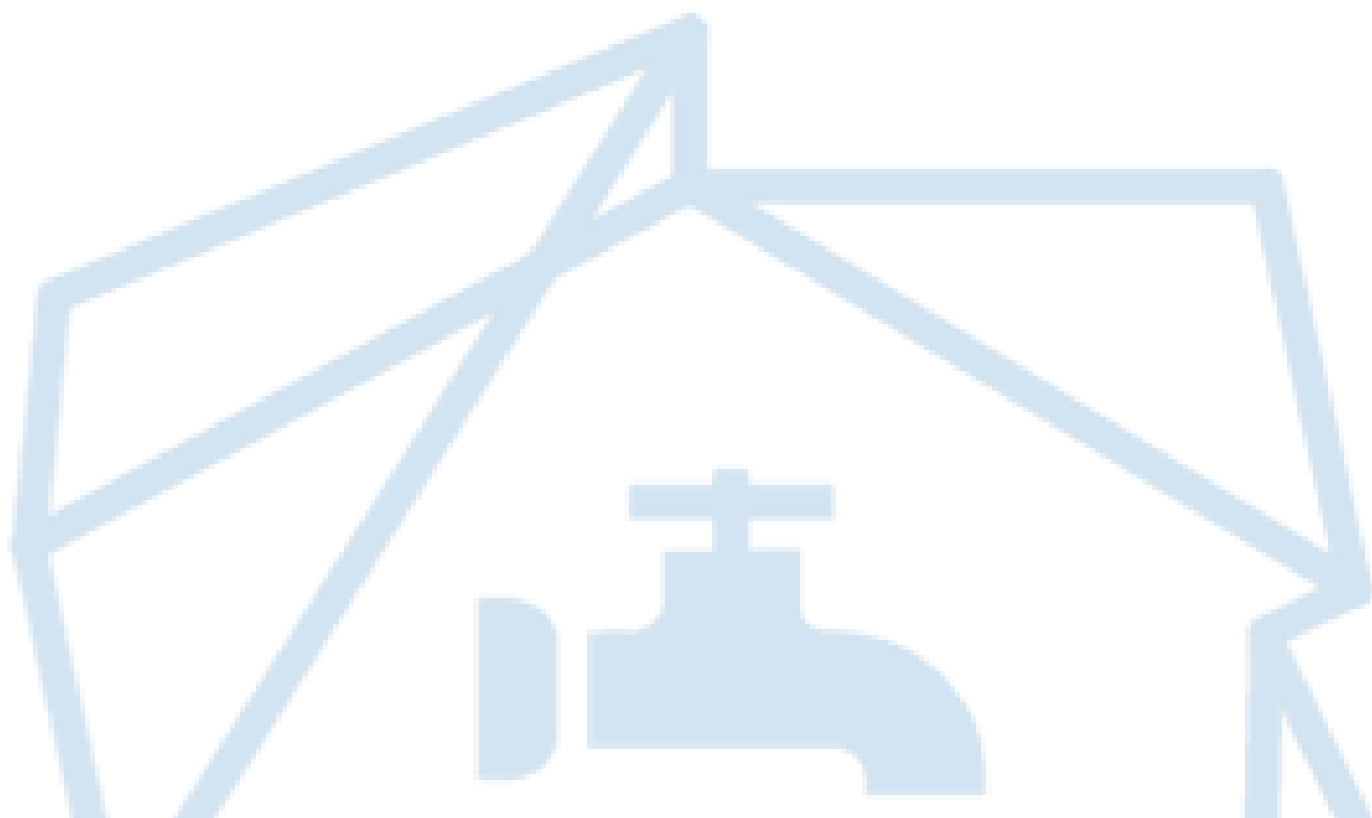
1. Zakres dla zadania 1 obejmuje dostawę urządzeń i niezbędnego oprogramowania:
 - 1) NGFW z pełną licencją enterprise do pracy w HA - 2 sztuki,
 - 2) NGFW z licencją enterprise dla OT – 3 sztuki,
 - 3) Switche zarządzalne dla IT – 7 szt. w tym:
 - a) Switche zarządzalne klasy Enterprise – 2 sztuki,
 - b) switche zarządzalne klienckie na potrzeby infrastruktury dostępowej-5 sztuk,
 - 4) Switche zarządzalne dla OT -3 sztuki
 - 5) Serwer kopii zapasowych NAS - 2 sztuki
 - 6) System MFA -system uwierzytelniania, autoryzacji i kontroli dostępu,
 - 7) Szafy rack do systemów bezpieczeństwa - 2 sztuki
 - 8) UPS do systemów cyberbezpieczeństwa - 1 sztuka
 - 9) Ponadto dla całości zadania wymagane jest wdrożenie u Zamawiającego wszystkich dostarczonych urządzeń i systemów.
2. Zakres dla zadania 2 obejmuje dostawę oprogramowania na potrzeby cyberbezpieczeństwa w tym:
 - 1) Platformy SIEM,
 - 2) Oprogramowania EDR/XDR do integracji z SIEM,
 - 3) Niezbędnych komponentów licencyjnych i integracyjnych,
 - 4) Wykonanie instalacji, uruchomienia i konfiguracji u Zamawiającego dostarczonego oprogramowania na potrzeby cyberbezpieczeństwa
 - 5) Wykonanie dokumentacji, szkoleń oraz wsparcia powdrożeniowego.

3. W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać każdorazowo z wyrazami „lub równoważne”. Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w 2025 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie „fabrycznie nowy” należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez „wadę fizyczną” należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia. Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu w standardowe oprogramowanie systemowe (firmware/OS urządzenia), z wyłączeniem licencji funkcjonalnych o charakterze czasowym.
- 1) Zamawiający wymaga, aby oferowany sprzęt, oprogramowanie oraz wszelkie ich komponenty:
 - a) nie pochodziły od dostawców uznanych decyzją właściwego organu za dostawców wysokiego ryzyka w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa KSC2,
 - b) były zgodne z obowiązującymi przepisami prawa krajowego i unijnego w zakresie cyberbezpieczeństwa,
 - 2) Oferowany sprzęt musi być dopuszczony do obrotu i użytkowania na terenie Unii Europejskiej, nie może podlegać sankcjom ani embargom oraz musi posiadać deklarację zgodności CE, o ile jest ona wymagana przepisami prawa.
 - 3) Oferowany sprzęt musi być urządzeniem sprzętowym (appliance), dedykowanym do pracy ciągłej w trybie 24/7.
 - 4) Dostarczane oprogramowanie musi być legalne, wolne od jakichkolwiek wad prawnych i technicznych, kompletne, w pełni sprawne oraz pochodzić z oficjalnego kanału dystrybucyjnego producenta lub uprawnionego podmiotu. Oprogramowanie musi być objęte odpowiednimi licencjami umożliwiającymi Zamawiającemu jego użytkowanie zgodnie z przeznaczeniem, co najmniej przez okres technicznej możliwości jego używania, chyba że w SOPZ wskazano inaczej. Przez „wadę techniczną” należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia
 - 5) O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

Zadanie 1

Spis treści

1.	WDROŻENIE WSZYSTKICH SYSTEMÓW	4
2.	NGFW Z PEŁNĄ LICENCJĄ ENTERPRISE DO PRACY W HA – 2 SZT.	7
3.	SERWER KOPII ZAPASOWYCH – 2 SZT.	19
4.	SWITCHE ZARZĄDZALNE – 7 SZT.	21
5.	SYSTEM MFA - SYSTEM UWIERZYTELNIANIA, AUTORYZACJI I KONTROLI DOSTĘPU	26
6.	NGFW Z LICENCJĄ ENTERPRICE DLA OT – 3 SZT.	29
7.	SWITCH ZARZĄDZALNY DLA OT – 3 SZT.	39
8.	SZAFA RACK DO SYSTEMÓW BEZPIECZEŃSTWA – 2 SZT.	41
9.	UPS DO SYSTEMÓW CYBERBEZPIECZEŃSTWA – 1 SZT.	42



1. Wdrożenie wszystkich systemów

1.1 Zakres ogólny wdrożenia

W ramach zamówienia Wykonawca zobowiązany będzie do wykonania kompleksowego wdrożenia dostarczonego systemu cyberbezpieczeństwa, obejmującego wszystkie elementy określone w niniejszym SOPZ. Wdrożenie powinno zakończyć się uruchomieniem produkcyjnym i przekazaniem Zamawiającemu w pełni działającego systemu zgodnego z wymaganiami SOPZ.

1.2 Etapy wdrożenia - Wdrożenie powinno obejmować co najmniej następujące etapy:

1.2.1 Analiza przedwdrożeniowa - Wykonawca powinien wykonać analizę środowiska Zamawiającego, obejmującą co najmniej:

- a) topologię sieci IT i OT,
- b) istniejące połączenia WAN,
- c) sposób dostępu zdalnego,
- d) zakres sieci VLAN i stref bezpieczeństwa,
- e) wymagania w zakresie VPN, NAC, MFA oraz segmentacji.

Efektem powinien być plan wdrożenia, który zostanie przedstawiony Administratorom IT Zamawiającego w formie zdalnej lub stacjonarnej. Plan powinien zostać zaakceptowany przez Zamawiającego przed rozpoczęciem konfiguracji.

1.2.2 Instalacja i uruchomienie sprzętu przez Wykonawcę

- a) montaż urządzeń w szafach RACK,
- b) podłączenie zasilania i okablowania,
- c) wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
- d) zapewnienie niezbędnego okablowania potrzebnego do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
- e) zapewnienie niezbędnych wkładek dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem stworzenia połączeń sieci LAN pomiędzy przełącznikami.
- f) połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
- g) wstępna konfiguracja sprzętu,
- h) aktualizacja firmware i systemów operacyjnych do wersji produkcyjnych.

1.2.3 Konfiguracja systemów bezpieczeństwa IT - Wykonawca skonfiguruje:

- a) klaster NGFW IT w trybie HA,
- b) polityki firewall, NAT, VPN, IPS, AV, Web Filtering, Application Control,
- c) SD-WAN, routing dynamiczny, agregację łączy,
- d) inspekcję SSL/TLS,
- e) system logowania i raportowania,
- f) integrację z Active Directory, MFA,
- g) zdalny dostęp VPN dla użytkowników.

1.2.4 Konfiguracja systemów bezpieczeństwa OT - Wykonawca skonfiguruje:

- a) NGFW OT wraz z politykami ruchu przemysłowego,
- b) ochronę SCADA, IPS dla OT,
- c) segmentację sieci OT,
- d) połączenia VPN OT-IT,
- e) monitoring i logowanie.

1.2.5 Konfiguracja przełączników - Wykonawca skonfiguruje:

- a) VLANy, routing, agregację,
- b) 802.1x,
- c) integrację z systemem MFA,
- d) polityki dostępu do sieci,

1.2.6 Konfiguracja systemu ochrony stacji roboczych i VPN - Wykonawca:

- a) uruchomi centralny serwer zarządzania,
- b) przygotuje paczki instalacyjne,
- c) wdroży ochronę i VPN na minimum 25 stacjach,
- d) skonfiguruje MFA,
- e) uruchomi centralne logowanie.

1.2.7 Konfiguracja systemu kopii zapasowych - Wykonawca:

- a) uruchomi serwer backupowy,
- b) skonfiguruje wolumeny, RAID, szyfrowanie,
- c) skonfiguruje harmonogramy backupów oraz deduplikację,
- d) przetestuje odtwarzanie danych.

1.3 Działania powdrożeniowe –**Wykonawca przedstawi:**

- a) konfigurację urządzeń,
- b) polityki bezpieczeństwa,
- c) instrukcję administracyjną,
- d) procedury awaryjne,

Wykonawca zapewni:

- a) obsługę zgłoszeń dotyczących prawidłowości funkcjonowania wdrożonych urządzeń i rozwiązań technicznych, nie wad gwarancyjnych.

- b) pomoc przy konfiguracji i eksploatacji dostarczonych rozwiązań,
- c) reagowanie na incydenty oraz usuwanie nieprawidłowości działania wynikających z błędów konfiguracyjnych lub eksploatacyjnych, z wyłączeniem wad objętych gwarancją.
- d) bieżące doradztwo w zakresie cyberbezpieczeństwa środowiska IT/OT Zamawiającego.

Wsparcie powdrożeniowe finansowane w ramach projektu „Cyberbezpieczne Wodociągi” będzie realizowane wyłącznie do dnia określonego przez grantodawcę jako okres kwalifikowalności wydatków, zgodnie z zasadami kwalifikowalności kosztów określonymi w regulaminie programu.

Zamawiający zastrzega, że po wyznaczonym przez grantodawcę terminu realizacji grantu, projekt „Cyberbezpieczne Wodociągi” nie będzie finansował żadnych świadczeń związanych z utrzymaniem, wsparciem lub rozwojem systemu, niezależnie od okresu obowiązywania gwarancji.

1.4 Gwarancja - wymogi ogólne.

- a) Oferowane urządzenia muszą posiadać standardową gwarancję producenta, wliczoną w cenę zakupu urządzenia, obejmującą usuwanie wad sprzętowych zgodnie z warunkami producenta. Okres standardowej gwarancji producenta nie może być krótszy niż 12 miesięcy od dnia podpisania protokołu odbioru końcowego.
- b) Gwarancja producenta jako element wliczony w cenę urządzenia, nie stanowi odrębnego kosztu kwalifikowanego projektu.
- c) Wykonawca udzieli gwarancji na wykonane prace instalacyjno-uruchomieniowe oraz konfigurację systemów na okres 12 miesięcy od dnia podpisania protokołu odbioru końcowego.
- d) Gwarancja obejmuje usuwanie wad i nieprawidłowości wynikających z nienależytego wykonania prac lub błędnej konfiguracji i nie stanowi odrębnego świadczenia odpłatnego.
- e) Świadczenia realizowane w ramach gwarancji po że po wyznaczonym przez grantodawcę terminie realizacji grantu nie będą finansowane ze środków grantu i zostaną wykonane w ramach wynagrodzenia określonego w umowie bez dodatkowych kosztów po stronie po stronie projektu grantowego.
- f) Po zakończeniu okresu finansowania grantu Zamawiający dopuszcza możliwość kontynuacji wsparcia systemu na podstawie odrębnej umowy, zawartej na zasadach rynkowych.
- g) Zamawiający zastrzega, że wszelkie koszty kwalifikowane w ramach grantu obejmują wyłącznie okres do dnia określonego jako termin realizacji grantu., a realizacja świadczeń po tej dacie nie będzie powodowała powstania zobowiązań finansowych po stronie projektu grantowego.
- h) Szczegółowe opisy wymogów w zakresie gwarancji zostały opisane w rozdziałach opisujących szczegółowe parametry techniczne dla poszczególnych pozycji.

1.5 Ofertowanie:

1.5.1 Wykonawca powinien w formularzu ofertowym przedstawić ofertę, która obejmuje kompleksową realizację zamówienia, w szczególności:

- a) dostawę urządzeń i oprogramowania,
- b) wdrożenie i konfigurację rozwiązań,
- c) udzielenie gwarancji na wykonane prace i wdrożone rozwiązania, stanowiącej element umowy i niewiążącej się z odrębnym wynagrodzeniem,
- d) zapewnienie wsparcia producenta oraz subskrypcji,
- e) zapewnienie wsparcia powdrożeniowego do dnia wyznaczonego przez grantodawcę jako terminu realizacji grantu.
- f) szkolenie specjalistyczne powdrożeniowe dla ASI

1.5.2 Cena oferty ma charakter ryczałtowy i obejmuje wszelkie koszty związane z prawidłową realizacją zamówienia, w tym w szczególności koszty:

- a) zakupu urządzeń oraz nabycia licencji,
- b) standardowych gwarancji producenta wliczonych w cenę urządzeń,
- c) wdrożenia, konfiguracji i uruchomienia systemów,
- d) wsparcia producenta oraz subskrypcji wymaganych w okresie realizacji projektu,
- e) wsparcia powdrożeniowego realizowanego do dnia wyznaczonego przez grantodawcę jako terminu realizacji grantu.

1.5.3 Elementy zamówienia o charakterze czasowym, w szczególności wsparcie producenta, subskrypcje oraz wsparcie powdrożeniowe, należy wycenić wyłącznie w zakresie przypadającym na okres do dnia wyznaczonego przez grantodawcę jako terminu realizacji grantu.

1.5.4 Świadczenia realizowane po dniu wyznaczonym przez grantodawcę jako terminu realizacji grantu, w tym realizacja gwarancji, nie podlegają odrębnemu wynagrodzeniu i są wykonywane w ramach ceny oferty albo zgodnie z warunkami standardowej gwarancji producenta.

1.5.5 Zamawiający nie dopuszcza wyodrębniania w ofercie pozycji kosztowych dotyczących świadczeń realizowanych po dniu wyznaczonym przez grantodawcę jako terminu realizacji grantu.

1.5.6 W przypadku, gdy producent oferuje standardowo dłuższe okresy gwarancji lub wsparcia, Zamawiający dopuszcza ich realizację bez wpływu na cenę oferty.

1.5.7 Zamawiający dopuszcza budowę systemu w oparciu o rozwiązania równoważne, pod warunkiem spełnienia minimalnych funkcjonalności określonych w SOPZ przy zachowaniu pełnej spójności technologicznej i interoperacyjności.

1.5.8 W przypadku zaoferowania rozwiązań równoważnych lub pochodzących od różnych producentów, Wykonawca musi zapewnić dla nich jednolity, centralny punkt wsparcia technicznego.

1.5.9 Wykonawca zobowiązany jest do oznakowania dostarczonego sprzętu oraz dokumentacji projektowej logotypami (K.PO, barwy narodowe, UE NextGenerationEU) zgodnie z Księgą Identyfikacji Wizualnej KPO.

2. NGFW z pełną licencją enterprise do pracy w HA – 2 szt.**2.1 Wymagania Ogólne**

System bezpieczeństwa powinien realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub

komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej powinny być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

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

System powinien umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System powinien wspierać protokoły IPv4 oraz IPv6 w zakresie:

- a) Firewall.
- b) Ochrony w warstwie aplikacji.
- c) Protokołów routingu dynamicznego.

2.2 Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – powinna istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System powinien umożliwiać agregację linków statycznych oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

2.3 Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall powinien dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
 - a) 10 portami Gigabit Ethernet RJ-45.
 - b) 8 gniazdami SFP 1 Gbps.
 - c) 4 gniazdami SFP+ 10 Gbps.
2. System Firewall powinien posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall powinien pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System powinien być wyposażony w zasilanie 230 VAC.

2.4 Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 5 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

2.5 Funkcje Systemu Bezpieczeństwa:

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

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

2.6 Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System powinien realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - a) Translację jeden do jeden oraz jeden do wielu.
 - b) Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.
3. W ramach systemu powinna istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall powinna umożliwić filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall powinien się integrować z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - a) Amazon Web Services (AWS).
 - b) Microsoft Azure.
 - c) Cisco ACI.
 - d) Google Cloud Platform (GCP).
 - e) OpenStack.
 - f) VMware NSX.
 - g) Kubernetes.

2.7 Połączenia VPN

1. System powinien umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewniać:
 - a) Wsparcie dla IKE v1 oraz v2.
 - b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - c) Obsługa protokołu Diffie-Hellman grup 19, 20.
 - d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - h) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - i) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - j) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - k) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - l) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania powinien posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie VPN jest dostępne jako opcja i nie jest wymagane w implementacji.

2.8 Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

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

2.9 Funkcje SD-WAN

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

2.10 Zarządzanie pasmem

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

2.11 Ochrona przed malware

1. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy powinien zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych powinna istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwiać konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System powinien umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System powinien dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System powinien współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System powinien zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Powinna istnieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.
10. Powinna istnieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

2.12 Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System powinien zapewnić wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Wymagane mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

2.13 Kontrola2.13 Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwić kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur.
6. Powinna istnieć możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).
7. System powinien dawać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

2.14 Kontrola WWW

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

2.15 Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall powinien umożliwiać weryfikację tożsamości użytkowników za pomocą:
 - a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System powinien dawać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System powinien umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie powinno być realizowane w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

2.16 Zarządzanie

1. Elementy systemu bezpieczeństwa powinny mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania powinna być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System powinien współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System powinien umożliwiać zarządzanie przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall powinien posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall powinien umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Powinna istnieć możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM) oraz możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

2.17 Logowanie

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

2.18 Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

2.19 Serwisy i licencje

2.19.1 Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen od dnia aktywacji na 36 miesięcy bez konieczności ponoszenia przez Zamawiającego dodatkowych opłat.

2.19.2 Subskrypcje muszą obejmować co najmniej następujące funkcjonalności (w zakresie zgodnym z ofertą producenta):

- a) aktualizacje sygnatur bezpieczeństwa (IPS, AV, Application Control),

- b) aktualizacje baz reputacyjnych adresów IP, domen i URL,
- c) Web Filtering,
- d) Antywirus oraz ochrona przed malware,
- e) system zapobiegania włamaniom (IPS),
- f) inspekcję ruchu szyfrowanego SSL/TLS (jeżeli jest wymagana w SOPZ),
- g) dostęp do poprawek bezpieczeństwa (security fixes) oraz aktualizacji oprogramowania systemowego (firmware).

2.19.3 Subskrypcje muszą:

- a) pochodzić z oficjalnego kanału dystrybucyjnego producenta lub autoryzowanego partnera,
- b) być wolne od wad prawnych,
- c) umożliwiać Zamawiającemu pełne korzystanie z funkcjonalności firewall zgodnie z SOPZ.

2.19.4 Subskrypcje oprogramowania dla firewall muszą zapewniać nieprzerwane i legalne użytkowanie systemu co najmniej przez 36 miesięcy. Koszt poniesiony ze środków własnych Zamawiającego poniesiony zostanie do dnia określonego przez grantodawcę jako okres realizowalności projektu., tj. przez cały okres kwalifikowalności kosztów w projekcie „Cyberbezpieczne Wodociągi”.

2.19.5 Ponieważ model licencjonowania producentów przewiduje subskrypcje o okresie obowiązywania dłuższym niż okres kwalifikowalności projektu:

- a) Zamawiający dopuszcza dostarczenie subskrypcji obejmujących okres wykraczający poza dzień określony jako okres kwalifikowalności projektu:
- b) do kosztów kwalifikowanych projektu zaliczona zostanie wyłącznie część kosztu subskrypcji proporcjonalnie przypadająca na okres do dnia określonego jako okres kwalifikowalności projektu.,
- c) pozostała część kosztu subskrypcji finansowana będzie ze środków własnych Zamawiającego.

2.19.6 Zamawiający nie dopuszcza wyodrębniania w ofercie ani osobnej wyceny kosztów subskrypcji, wsparcia producenta ani aktualizacji przypadających po dniu określonym jako okres kwalifikowalności projektu.

2.19.7 Subskrypcje:

- a) nie mogą być uzależnione od obowiązku zawarcia dodatkowych umów po zakończeniu projektu,
- b) nie mogą powodować powstania zobowiązań finansowych po stronie projektu grantowego po dniu określonym jako okres kwalifikowalności projektu

2.19.8 Wsparcie producenta oraz subskrypcje realizowane po dniu określonym jako okres kwalifikowalności projektu

- a) nie stanowią kosztów kwalifikowanych projektu „Cyberbezpieczne Wodociągi”,
- b) mogą być kontynuowane wyłącznie na podstawie odrębnej umowy, zawartej na zasadach rynkowych.

2.20 Gwarancja.

- 1) Oferowane urządzenia muszą być fabrycznie nowe i objęte standardową gwarancją producenta, wliczoną w cenę zakupu urządzenia.
- 2) Okres standardowej gwarancji producenta nie może być krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru końcowego.
- 3) Gwarancja producenta obejmuje w szczególności:
 - a) usuwanie wad sprzętowych,
 - b) naprawę lub wymianę uszkodzonych komponentów na nowe lub równoważne,
 - c) dostęp do aktualizacji oprogramowania systemowego (firmware) niezbędnych do prawidłowego i bezpiecznego funkcjonowania urządzenia.
- 4) Gwarancja powinna być realizowana jest przez producenta lub autoryzowanego partnera serwisowego, w trybie:
 - a) NBD (Next Business Day) lub
 - b) on-site w siedzibie Zamawiającego – zgodnie ze standardowymi warunkami producenta.
- 5) Gwarancja producenta:

- a) stanowi integralny element urządzenia,
 - b) nie jest usługą odrębną,
 - c) nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi”.
- 6) Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej.
Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
- 7) Realizacja gwarancji po dniu 30.06.2026 r. nie powoduje powstania zobowiązań finansowych po stronie projektu grantowego i odbywa się zgodnie z warunkami standardowej gwarancji producenta.

2.21 Dodatkowa licencja systemu kompatybilnego z oferowanym NGFW:

System zarządzania zdalnym dostępem VPN i ochrony dla stacji roboczych wraz z serwerem centralnego zarządzania.

W ramach postępowania wymagany jest dostarczenie dodatkowej licencji rozwiązania do zarządzania konfiguracją dostępu VPN i ochrony dla stacji roboczych wraz z mechanizmami centralnego zarządzania. Dostarczone rozwiązanie powinno zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się, aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

2.22 Parametry systemu zarządzania dostępem VPN i ochrony dla stacji roboczych.

1. Elementy systemu zarządzania dostępem i ochrony dla stacji roboczych powinny zawierać następujące funkcje i mechanizmy:
 - 1) Kontrola antywirusowa
 - a) Mechanizmy Anti-Ransomware pozwalające na behawioralne wykrywanie podejrzanej aktywności złośliwego oprogramowania typu Ransomware
 - b) Mechanizm Antiexploit pozwalający na ochronę popularnych aplikacji przed atakami typu 0-day
 - c) Możliwość blokowania podejrzanych adresów URL i niebezpiecznych stron
 - d) Mechanizmy antywirusowe oparte o:
 - Sygnaturach aktualizowanych min. co godzinę
 - Baz reputacji plików opartych o funkcję skrótu dostępnych on-line i działających w czasie rzeczywistym
 - Możliwości integracji z systemami typu sandbox w chmurze oraz on-prem, wraz z możliwością zarówno wysyłania plików jak i korzystania z informacji o wykrytych zagrożeniach
 - 2) Kategoryzacja URL
 - a) URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
 - b) Możliwość integracji z wtyczką do przeglądarki internetowej, celem analizy kategorii WWW dla ruchu SSL/HTTPS
 - 3) Analiza podatności
 - a) Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
 - b) Mechanizmy pozwalające na wymuszenie aktualizacji systemu lub popularnych aplikacji
 - 4) Dostęp VPN
 - a) Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - b) Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.

- c) Rozwiązanie powinno umożliwiać realizowanie funkcjonalności split tunneling w oparciu o aplikacje, przykładowo musi istnieć możliwość wykluczenia aplikacji wymagających dużej ilości pasma np.: Microsoft Office 365, Microsoft Teams, Skype, GoToMeeting, Zoom, WebEx, YouTube
 - d) Rozwiązanie powinno umożliwiać realizowanie funkcjonalności split tunneling w oparciu o domenę (FQDN)
 - e) Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
 - f) Mechanizmy uwierzytelniania dwuskładnikowego.
 - g) System powinien umożliwiać zastosowanie protokołu SAML dla SSL VPN
- 2. Funkcjonalność kontroli i blokowania urządzeń USB
 - 3. Kontrola ruchu sieciowego
 - 1) Kontrola ruchu sieciowego pochodzącego z aplikacji - w oparciu o wbudowany Firewall aplikacyjny.
 - 4. Centralne logowanie i raportowanie
 - 1) System powinien umożliwiać wysyłanie logów ze stacji roboczych do centralnego systemu logowania i raportowania
 - 5. Centralne zarządzanie
 - 1) System powinien umożliwiać centralne zarządzania stacjami roboczymi
 - 6. Poszczególne mechanizmy powinny być dostępne dla następujących wersji systemów operacyjnych Windows oraz Mac OS: Microsoft Windows 11 (64-bit), Microsoft Windows 10 (32-bit, 64-bit), Windows Server 2025, Windows Server 2022, Windows Server 2016

2.23 Parametry systemu centralnego zarządzania.

- 1. Elementy wchodzące w skład systemu powinny być zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2016, Microsoft Windows Server 2022, Microsoft Windows Server 2025, lub Ubuntu 22.04 LTS Server and Desktop
- 2. System powinien umożliwiać automatyczną aktualizację oprogramowania na urządzeniach końcowych oraz powinien zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox
- 3. Ponadto powinien zapewniać:
 - 3.1. Integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD.
 - 3.2. Definiowanie różnych profili (wersji konfiguracji) dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie.
 - 3.3. Zautomatyzowany proces zarządzania aplikacją kliencką.
 - 3.4. Przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS, w których administrator może określić komponenty instalatora dla stacji roboczych przynajmniej takie jak:
 - a) filtrowanie URL,
 - b) analiza podatności,
 - c) application firewall
 - d) antywirus
 - 3.5. Możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym.
 - 3.6. Panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych.
 - 3.7. Panel, w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych: System powinien umożliwiać wyświetlanie w konsoli zarządzania informacji o stacjach roboczych, które mogą służyć do diagnozy problemów oraz stanu stacji min:
 - a) Typ połączenia (Ethernet/Wifi)

- b) Adres IP
 - c) Adres IP domyślnej bramy
 - d) Adres MAC
 - e) Adres MAC bramy sieciowej
 - f) Nazwa sieci WiFi (SSID)
 - g) Model sprzętu
 - h) Producent sprzętu
 - i) Informacje o procesorze
 - j) Informacje o pamięci RAM
 - k) Numer seryjny
 - l) Informacje o dysku twardym (rozmiar)
- 3.8. Możliwość wymuszenia aktualizowania systemu i aplikacji z racji wykrytych podatności na stacjach roboczych.
- 3.9. Automatyczne wykrywanie stacji klienckich w grupach roboczych.
System powinien umożliwiać określanie czy dana stacja znajduje się w wewnętrznej sieci chronionej, czy poza nią, na podstawie reguł budowanych w oparciu cechy:
- a) Parametrów DHCP
 - b) Serwerów DNS
 - c) Połączenia ze stacją zarządzającą
 - d) Adresacją sieci
 - e) Bramą domyślną (Default Gateway) (adres IP lub adres MAC)
 - f) Publiczny adres IP
 - g) Tunel VPN
 - h) Dostępny IP za pomocą PING
 - i) Typ połączenia (Ethernet lub WiFi)
- 3.10. Reguły określające czy stacja należy do sieci zaufanej powinny być budowane w oparciu o różne kombinacje powyższych parametrów.
- 3.11. Reguły powinny pozwalać na przydzielenie różnych profili bezpieczeństwa zależnie od określenia przynależności do sieci zaufanej.
- 3.12. Logowanie zdarzeń z aplikacji klienckich powinno posiadać możliwość ich przeglądania z funkcją filtrów oraz możliwością pobierania logów przez administratora.
- 3.13. Powinny być realizowane następujące funkcjonalności:
- 3.13.1 Generowanie alarmów: związanych z zarządzaniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach.
- 3.13.2 Definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcją przypisywania uprawnień do elementów panelu konfiguracyjnego.
- 3.13.3 Zarządzanie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN.
- 3.13.4 Automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji.
- 3.13.5 Możliwość przeniesienia stacji/urządzenia do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi.
- 3.13.6 Możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
- 3.13.7 Możliwość skonfigurowania weryfikacji zgodności (posture check) w celu sprawdzenia czy na stacji końcowej jest:
- a) Uruchomiony AV i powinien mieć zaktualizowaną bazę,
 - b) Zainstalowaną odpowiednią wersję systemu operacyjnego,
 - c) Uruchomiony odpowiedni proces,
 - d) Zainstalowany odpowiedni Certyfikat,

- e) Odpowiedni wpis w rejestrach systemowych,
 - f) Stworzony odpowiedni plik,
 - g) Użytkownika zalogowanego do konkretnej domeny AD,
- 3.14. Administrator powinien mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy systemu.
- 3.15. Centralny system zarządzania powinien zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpiezonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

2.24 Licencje oraz serwisy.

W ramach postępowania wraz z konsolą centralnego zarządzania powinny zostać dostarczone niezbędne licencje upoważniające do zainstalowania i centralnego zarządzania 25 aplikacjami klienckimi na stacjach roboczych. Licencja ma charakter czasowy i powinna obowiązywać przez okres 36 miesięcy od daty wdrożenia. Do dofinansowania zgłoszona została wyłącznie część kosztu licencji proporcjonalnie przypadająca na okres kwalifikowalności projektu, tj. po dniu określonym jako okres kwalifikowalności projektu. Pozostała część kosztu licencji zostanie sfinansowana ze środków własnych Zamawiającego (beneficjenta).

1. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować funkcjonalności:
 - a) Filtrowanie adresów URL oraz filmów wideo,
 - b) Możliwość zarządzania stacjami roboczymi i profilami SSL i IPSec VPN,
 - c) Możliwość wykonywania analizy podatności systemów operacyjnych i zainstalowanych aplikacji,
 - d) Centralne zarządzanie politykami bezpieczeństwa i konfiguracją VPN,
 - e) Centralne logowanie i raportowanie zdarzeń,
 - f) Integrację z systemami uwierzytelniania, w tym MFA,
 - g) Aktualizacje baz sygnatur, reguł bezpieczeństwa i komponentów systemowych,
2. Licencja powinna obejmować:
 - a) dostęp do aktualizacji oprogramowania,
 - b) dostęp do poprawek bezpieczeństwa (security fixes),
 - c) wsparcie techniczne producenta lub autoryzowanego partnera producenta.
3. Pochodzenie licencji:
 - a) musi pochodzić z oficjalnego kanału dystrybucyjnego producenta lub autoryzowanego partnera,
 - b) musi być wolna od wad prawnych,
 - c) nie może być uzależniona od obowiązku zawarcia dodatkowych umów po zakończeniu projektu.

3. Serwer kopii zapasowych – 2 szt.

PARAMETR	WYMAGANIA MINIMALNE
Procesor	Wielordzeniowy procesor osiągający wynik minimum 7500 punktów w teście PassMark.
Obudowa	Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie.
Pamięć RAM	Minimum 8GB ECC UDIMM z możliwością rozbudowy do minimum 32GB.
Ilość obsługiwanych dysków	Minimum 12 dysków o maksymalnej pojemności dysku nie mniejszej niż 12TB każdy, po podłączeniu modułów rozszerzających minimum 24 dyski.
Zainstalowane dyski	Minimum 6 dysków o pojemności 12TB każdy, zgodnych z listą kompatybilności oferowanego serwera NAS oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1,2 miliona, - możliwość aktualizacji oprogramowania dysków HDD bezpośrednio z poziomu systemu operacyjnego serwera NAS podczas pracy.
Interfejsy sieciowe	Minimum 2 porty 1GbE RJ-45. Minimum 1 port 10GbE RJ-45. Obsługa agregacji łączy. Możliwość rozbudowy o dodatkową kartę sieciową z portami 10GbE SFP+.
Porty	Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.
Wskaźniki LED	Status, HDD, zasilanie, LAN
Obsługa RAID	Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	SMB, NFS, FTP, WebDAV, iSCSI, SSH, SNMP
Usługi	1. Serwer VPN, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer WWW, Serwer plików, Manager plików przez WebUI, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Możliwość utworzenia klastra wysokiej dostępności (<i>ang. High Availability Cluster</i>) pracującego minimum w trybie aktywny - pasywny. Klaster powinien obsługiwać w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. W skład klastra powinny wchodzić co najmniej 2 urządzenia. Drugie urządzenie zostanie zakupione z Środków własnych Zamawiającego.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski

PARAMETR	WYMAGANIA MINIMALNE
Gwarancja i serwis	Oferowane urządzenia powinny być objęte gwarancją producenta na okres 36 miesięcy, liczony od daty odbioru końcowego. Zamawiający zakłada, że gwarancja jest nadawana automatycznie przez producenta i stanowi standardowy, nieodczynny element zakupywanego sprzętu i nie jest odrębnym kosztem. W przypadku gdy oferowany sprzęt umożliwia wyszczególnienie gwarancji jako osobną pozycję, Wykonawca powinien określić jej koszt jako odrębny w formularzu ofertowym i uwzględnić osobno koszt zakupu na okres do 30.06.2026 r. (zgodnie z kwalifikowalnością w gracie) oraz od 30.06.2026 do końca trwania 36-miesięcznej gwarancji.
Waga	Maksymalnie 16 kg (bez dysków).
Typowy pobór mocy podczas pracy	Maksymalnie 300W
Certyfikaty	Minimum CE
System plików	Dyski wewnętrzne: BTRFS lub inny równoważny
Szyfrowanie	Mechanizm szyfrowania sprzętowego
Zasilacz	Redundantny zasilacz o mocy pozwalającej na bezproblemową pracę serwera NAS w przypadku awarii jednego z modułów.
Chłodzenie	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy.

Warunki gwarancji dla serwera:

- Oferowany serwer musi być fabrycznie nowy i objęty standardową gwarancją producenta, wliczoną w cenę zakupu urządzenia.
- Okres standardowej gwarancji producenta na serwer nie może być krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru końcowego.
- Gwarancja producenta obejmuje w szczególności:
 - usuwanie wad sprzętowych,
 - naprawę lub wymianę uszkodzonych komponentów na nowe lub równoważne,
 - dostęp do aktualizacji firmware'u oraz mikrokodu producenta.
- Gwarancja powinna być realizowana jest w trybie:
 - serwisu producenta lub autoryzowanego partnera serwisowego,
 - on-site w siedzibie Zamawiającego lub w trybie NBD (Next Business Day).
- Gwarancja producenta:
 - stanowi integralny element urządzenia,
 - nie jest usługą odrębną,
 - nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi”.
- Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej. Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
- Realizacja gwarancji po dniu określonym przez grantodawcę jako termin kwalifikowalności projektu. nie powoduje powstania zobowiązań finansowych po stronie projektu grantowego i odbywa się zgodnie z warunkami standardowej gwarancji producenta.

4. Switche zarządzalne – 7 szt.

4 A. Switche Zarządzalne IT – 5 szt.

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu powinny zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym NGFW z poz. 2, o następujących parametrach:

4.1 Parametry fizyczne platformy

- 4.1.1 Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- 4.1.2 Zasilanie AC 230V.
- 4.1.3 Maksymalny pobór mocy: 60 W.
- 4.1.4 Minimalny zakres temperatury pracy: 0-40°C.

4.2 Interfejsy sieciowe - wymagania minimalne

- 4.2.1 Wymagany jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - a) 48 porty GE RJ-45.
 - e) 4 porty 10 GE SFP+

4.3 Zarządzanie

Funkcje zarządzania powinny posiadać następujące funkcjonalności:

- 4.3.1 Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- 4.3.2 Wsparcie dla SNMP w wersjach 1-3
- 4.3.3 Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- 4.3.4 Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- 4.3.5 Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- 4.3.6 Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- 4.3.7 Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- 4.3.8 Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- 4.3.9 Automatycznie wykonywane rewizje konfiguracji.

4.4 Parametry wydajnościowe

- 4.4.1 Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
- 4.4.2 Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- 4.4.3 Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

4.5 Wymagane funkcje

- 4.5.1 Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- 4.5.2 Obsługa Jumbo Frames.
- 4.5.3 Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- 4.5.4 Agregacja portów zgodna ze standardem 802.3ad.
- 4.5.5 Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- 4.5.6 Obsługa routingu statycznego.
- 4.5.7 Port-mirroring.
- 4.5.8 Uwierzytelnianie 802.1x na poziomie portu.
- 4.5.9 Uwierzytelnianie 802.1x w oparciu o adres MAC.
- 4.5.10 W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- 4.5.11 W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- 4.5.12 W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- 4.5.13 Obsługa protokołu sFlow.

4.6 Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

4.6.1 Przełączniki powinny wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny powinien zawierać co najmniej:

- 4.6.1.1 Centralne zarządzanie konfiguracją urządzenia.
- 4.6.1.2 Aktualizację oprogramowania realizowaną z systemu centralnego zarządzania.
- 4.6.1.3 Centralne zarządzanie sieciami VLAN.
- 4.6.1.4 Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
- 4.6.1.5 Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
- 4.6.1.6 Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
- 4.6.1.7 Integrację z systemem kontroli dostępu. Urządzenie powinno podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- 4.6.1.8 Automatyczną detekcję i rekomendacje konfiguracji.
- 4.6.1.9 Przesyłanie logów na zewnętrzny serwer syslog.
- 4.6.1.10 Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- 4.6.1.11 Obsługa białych i czarnych list adresów MAC.
- 4.6.1.12 Wykrywanie aplikacji komunikujących się w sieci.
- 4.6.2 Powinna być możliwość redundantnego połączenia z elementami zarządzającymi.
- 4.6.3 W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

4.7 Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- 4.7.1 System powinien realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- 4.7.2 System powinien zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

4.8 Gwarancja

- 1) Oferowane urządzenia muszą być fabrycznie nowe i objęte standardową gwarancją producenta, wliczoną w cenę zakupu urządzenia.
- 2) Okres standardowej gwarancji producenta nie może być krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru końcowego.
- 3) Gwarancja producenta obejmuje w szczególności:
 - a) usuwanie wad sprzętowych,
 - b) naprawę lub wymianę uszkodzonych komponentów na nowe lub równoważne,
 - c) dostęp do aktualizacji oprogramowania systemowego (firmware) niezbędnych do prawidłowego i bezpiecznego funkcjonowania urządzenia.
- 4) Gwarancja powinna być realizowana jest przez producenta lub autoryzowanego partnera serwisowego, w trybie:
 - a) NBD (Next Business Day) lub
 - b) on-site w siedzibie Zamawiającego – zgodnie ze standardowymi warunkami producenta.
- 5) Gwarancja producenta:
 - a) stanowi integralny element urządzenia,
 - b) nie jest usługą odrębną,
 - c) nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi”.
- 6) Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej. Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
- 7) Realizacja gwarancji po dniu 30.06.2026 r. nie powoduje powstania zobowiązań finansowych po stronie projektu grantowego i odbywa się zgodnie z warunkami standardowej gwarancji producenta.

4.B. Switche Zarządzalne klasy Enterprise – 2 szt.

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

4.b.1. Parametry fizyczne platformy

- a) Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- b) Zasilanie AC 230V.
- c) Wbudowany redundantny zasilacz.
- d) Maksymalny pobór mocy: 50 W.
- e) Minimalny zakres temperatury pracy: 0-50°C.

4.b.2. Interfejsy sieciowe - wymagania minimalne

1. Wymagany jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - a) 48 porty GE RJ-45.
 - e) 4 porty 10 GE SFP+.

4.b.3. Zarządzanie

- a) Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
- b) Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.

- c) Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- d) Wsparcie dla SNMP w wersjach 1-3
- e) Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- f) Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- g) Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- h) Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- i) Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- j) Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- k) Automatycznie wykonywane rewizje konfiguracji.

4.b.4 Parametry wydajnościowe

- a) Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.
- b) Tablica adresów MAC o pojemności co najmniej 32 k wpisów.
- c) Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

4.b.5. Wymagane funkcje

- a) Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- b) Obsługa Jumbo Frames.
- c) Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- d) Agregacja portów zgodna ze standardem 802.3ad.
- e) Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- f) Wsparcie dla Private VLAN.
- g) Obsługa routingu statycznego.
- h) Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
- i) Port-mirroring.
- j) Uwierzytelnianie 802.1x na poziomie portu.
- k) Uwierzytelnianie 802.1x w oparciu o adres MAC.
- l) W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- m) W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- n) W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- o) Obsługa protokołu sFlow.

4.b.6. Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- a) Centralne zarządzanie konfiguracją urządzenia
 - b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - c) Centralne zarządzanie sieciami VLAN.
 - d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - g) Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - h) Automatyczna detekcja i rekomendacje konfiguracji.
 - i) Przesyłanie logów na zewnętrzny serwer syslog.
 - j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - k) Obsługa białych i czarnych list adresów MAC.
 - l) Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

4.b.7. Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- a) System powinien realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- b) System powinien zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

4.b.8. Gwarancja oraz wsparcie

- 1) Oferowane urządzenia muszą być fabrycznie nowe i objęte standardową gwarancją producenta, wliczoną w cenę zakupu urządzenia.
- 2) Okres standardowej gwarancji producenta nie może być krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru końcowego.
- 3) Gwarancja producenta obejmuje w szczególności:
 - a) usuwanie wad sprzętowych,
 - b) naprawę lub wymianę uszkodzonych komponentów na nowe lub równoważne,
 - c) dostęp do aktualizacji oprogramowania systemowego (firmware) niezbędnych do prawidłowego i bezpiecznego funkcjonowania urządzenia.
- 4) Gwarancja powinna być realizowana jest przez producenta lub autoryzowanego partnera serwisowego, w trybie:
 - a) NBD (Next Business Day) lub
 - b) on-site w siedzibie Zamawiającego – zgodnie ze standardowymi warunkami producenta.
- 5) Gwarancja producenta:
 - a) stanowi integralny element urządzenia,
 - b) nie jest usługą odrębną,
 - c) nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi”.

- 6) Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej. Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
- 7) Realizacja gwarancji po dniu 30.06.2026 r. nie powoduje powstania zobowiązań finansowych po stronie projektu grantowego i odbywa się zgodnie z warunkami standardowej gwarancji producenta.

5. System MFA - System uwierzytelniania, autoryzacji i kontroli dostępu

5.1 Wymagania ogólne

5.1.1 Oferowane rozwiązanie powinno pozwalać na centralne zarządzanie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu powinien zapewniać wszystkie wymienione poniżej funkcje.

się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów. System zapewniać nie mniej niż:

5.1.3 Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności.

5.1.4 Posiadać graficzną reprezentację statusu uwierzytelnionych użytkowników.

5.1.5 Posiadać Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:

- a. Lokalnie,
- b. Zdalnie w oparciu o protokół Syslog.

5.1.6 Konfigurację Captive Portalu.

5.2 Parametry systemu

5.2.1 Poszczególne elementy wchodzące w skład systemu powinny zapewniać obsługę:

- a) 4 wirtualnych interfejsów sieciowych.
- b) możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje: 4, 5, 6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI.

5.1 Parametry wydajnościowe i licencyjne

5.1.1 System powinien obsługiwać co najmniej:

- a) Uwierzytelnianie dla 100 użytkowników.
- b) 5 lokalnych centrów certyfikacji (CA).
- c) Posiadać 25 tokenów dla uwierzytelniania dwuskładnikowego.
- d) Posiadać możliwość zdefiniowania co najmniej 10 grup użytkowników.

5.2 Wymagania funkcjonalne – uwierzytelnianie

Celem realizacji funkcji uwierzytelniających, system powinien zapewniać nie mniej niż:

- 5.2.1 Lokalną, wbudowaną bazę użytkowników.
- 5.2.2 Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo.
- 5.2.3 Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników.
- 5.2.4 Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV.
- 5.2.5 Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:

- a. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),
- b. czasu ważności hasła,
- 5.2.6 Konfigurowalną politykę blokowania kont, która będzie uwzględniać:
 - a. ilość nieudanych logowań,
 - b. czas blokowania konta,
 - c. okres nieaktywności, po którym konto jest blokowane.
- 5.2.7 Możliwość odzyskiwania haseł:
 - a. z wykorzystaniem adresu email,
 - b. z wykorzystaniem pytania pomocniczego.
- 5.2.8 Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system powinien oferować:
 - a. wbudowany serwer RADIUS,
 - b. integrację z zewnętrznymi serwerami RADIUS – praca jako klient.
- 5.2.9 Obsługę protokołu LDAP, w tym zakresie system powinien oferować:
 - a. wbudowany serwer LDAP,
 - b. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).
- 5.2.10 Obsługę protokołu SAML - Identity Provider (IdP) proxy.
- 5.2.11 Realizację funkcji SSO (Single Sign On) w oparciu o:
 - a. integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,
 - b. dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,
 - c. kontekst użytkownika przesyłany z serwera RADIUS,
 - d. informacje uzyskiwane poprzez protokół Syslog,

5.3 Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe

Realizując uwierzytelnianie dwuskładnikowe, system powinien zapewniać nie mniej niż:

- 5.3.1 Obsługę dla tokenów sprzętowych (hardware): tokeny powinny pochodzić od tego samego producenta co system uwierzytelniania.
- 5.3.2 Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.
- 5.3.3 Dla tokenów na system iOS i Android wymaga się:
 - a) aktywacji z centralnego systemu uwierzytelniania (seed provisioning),
 - b) możliwości konfiguracji ilości generowanych cyfr (6 lub 8),
 - c) generowania kodu (cyfr) co 30 lub 60 sekund,
 - d) możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
 - e) ochrony dostępu poprzez konfigurowalny kod PIN,

5.4 Możliwość integracji z logowaniem do systemu Windows.

5.4.1 Wymagania funkcjonalne – 802.1

System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

- 5.4.1.1 Obsługa co najmniej poniższych protokołów EAP:
 - a) PEAP,
 - b) EAP-TTLS,
 - c) EAP-TLS,
 - d) EAP-GTC.

5.4.1.2 Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication).

5.4.1.3 Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.

5.5 Wymagania funkcjonalne – zarządzanie certyfikatami

System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

- 5.5.1 Obsługę wbudowanego CA (Certificate Authority).
- 5.5.2 Obsługę CA pośredniczących (Intermediate CA).
- 5.5.3 Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego.
- 5.5.4 Możliwość pobrania wygenerowanych certyfikatów.
- 5.5.5 Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP.
- 5.5.6 Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP.
- 5.5.7 Możliwość generowania certyfikatów typu wildcard.
- 5.5.8 Realizacja CRL (Certificate Revocation List).
- 5.5.9 Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).
- 5.5.10 Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

5.6 Zarządzanie

- 5.6.1 Zarządzanie powinno być realizowane w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki.
- 5.6.2 System powinien udostępniać graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS.
- 5.6.3 Tworzenie kopii bezpieczeństwa konfiguracji powinno być realizowane z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć.
- 5.6.4 Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

5.7 Licencja

- 5.7.1 Licencja systemu MFA musi obejmować co najmniej 25 tokenów uwierzytelniających, umożliwiających realizację uwierzytelniania wieloskładnikowego (MFA) dla użytkowników i administratorów Zamawiającego.
- 5.7.2 Licencja nie może być uzależniona od:
 - a) obowiązku zawarcia po dniu 30.06.2026 r. dodatkowych umów,
 - b) obowiązku korzystania z infrastruktury zlokalizowanej poza UE w celu prawidłowego działania systemu.
- 5.7.3 W ramach licencji wymagane jest zapewnienie:
 - a) 25 aktywnych tokenów MFA,
 - b) możliwości swobodnego przypisywania tokenów do użytkowników,
 - c) możliwości dezaktywacji, ponownej aktywacji oraz ponownego przypisania tokenu innemu użytkownikowi bez konieczności nabywania dodatkowych licencji.
- 5.7.4 Tokeny MFA mogą mieć postać:
 - a) tokenów sprzętowych,
 - b) tokenów programowych (aplikacje mobilne),
 - lub kombinacji obu typów – zgodnie z ofertą producenta.
- 5.7.5 Licencja na tokeny MFA:
 - a) nie może być ograniczona liczbą logowań ani liczbą uwierzytelnień,
 - b) nie może być ograniczona czasowo krócej niż do dnia 30.06.2026 r.,
 - c) musi umożliwiać jednoczesne korzystanie z tokenów przez użytkowników.
- 5.7.6 Licencja musi obejmować prawo do:
 - a) generowania kodów jednorazowych (OTP),
 - b) uwierzytelniania w oparciu o token w procesach: VPN, dostęp administracyjny, 802.1x, aplikacje

- webowe (SAML),
- c) centralnego zarządzania tokenami z poziomu konsoli administracyjnej systemu MFA.
- 5.7.7 Licencja musi być:
- a) wolna od wad prawnych,
 - b) przenoszalna na Zamawiającego w zakresie użytkowania systemu,
 - c) zgodna z przepisami prawa krajowego i unijnego.
- 5.7.8 W przypadku gdy producent oferuje standardowo licencję obejmującą większą liczbę tokenów MFA, Zamawiający dopuszcza jej dostarczenie bez wpływu na cenę oferty.
- 5.7.9 Licencja na tokeny MFA:
- a) stanowi integralny element systemu MFA,
 - b) nie jest usługą odrębną,
 - c) nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi” poza okresem do dnia określonego przez grantodawcę jako okres kwalifikowalności projektu
- 5.7.10 Licencja musi zapewniać nieprzerwane, legalne korzystanie z systemu MFA co najmniej przez 36 miesięcy – do dofinansowania zgłoszony został proporcjonalny koszt do dnia określonego przez grantodawcę jako okres kwalifikowalności projektu
- 5.7.11 Licencja w okresie obowiązywania wykraczającym poza okres kwalifikowalności projektu, będzie finansowana ze środków własnych Zamawiającego.

6. NGFW z licencją enterprise dla OT – 3 szt.

6.1 Wymagania Ogólne

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

6.1.2 System realizujący funkcję Firewall powinien zapewnić pracę w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

6.1.3 System powinien umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

6.1.4 Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

6.1.5 System powinien wspierać protokoły IPv4 oraz IPv6 w zakresie:

- a) Firewall.
- b) Ochrony w warstwie aplikacji.
- c) Protokołów routingu dynamicznego.

6.2 Redundancja, monitoring i wykrywanie awarii

6.2.1 W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – powinna istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall powinien zapewniać funkcję synchronizacji sesji.

6.2.2 System powinien zapewniać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

6.2.3 System powinien zapewniać monitoring stanu realizowanych połączeń VPN.

6.2.4 System powinien umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto dawać możliwość tworzenia interfejsów redundantnych.

6.3 Interfejsy, Dysk, Zasilanie:

- 6.3.1 System realizujący funkcję Firewall'a powinien dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
- 10 portami Gigabit Ethernet RJ-45.
- 6.3.2 System Firewall powinien posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
- 6.3.3 System Firewall powinien pozwalać na skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- 6.3.4 System być wyposażony w zasilanie 230 AC.

6.4 Parametry wydajnościowe:

- 6.4.1 W zakresie Firewall'a powinna być realizowana obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 100 tys. nowych połączeń na sekundę.
- 6.4.2 Przepustowość Stateful Firewall powinna być nie mniejsza niż 10 Gbps dla pakietów 512 B.
- 6.4.3 Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji powinna być nie mniejsza niż 3.5 Gbps.
- 6.4.4 Wydajność szyfrowania IPsec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.
- 6.4.5 Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- powinna być minimum 2.4 Gbps.
- 6.4.6 Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - powinna być minimum 1.3 Gbps.
- 6.4.7 Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – powinna być minimum 1.4 Gbps.

6.5 Funkcje Systemu Bezpieczeństwa:

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

- 6.5.1 Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
- 6.5.2 Kontrola Aplikacji.
- 6.5.3 Poufność transmisji danych - połączenia szyfrowane IPsec VPN.
- 6.5.4 Ochrona przed malware.
- 6.5.5 Ochrona przed atakami - Intrusion Prevention System.
- 6.5.6 Kontrola stron WWW.
- 6.5.7 Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
- 6.5.8 Zarządzanie pasmem (QoS, Traffic shaping).
- 6.5.9 Powinno być realizowane dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
- 6.5.10 Powinna być realizowana inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
- 6.5.11 Powinna istnieć możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
- 6.5.12 Rozwiązanie powinno posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

6.6 Polityki Firewall

- 6.6.1 Polityka Firewall powinna uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- 6.6.2 System powinien realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.
- 6.6.3 W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN
- 6.6.4 Powinna istnieć możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
- 6.6.5 Polityka firewall powinna umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
- 6.6.6 Powinna istnieć możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
- 6.6.7 Element systemu realizujący funkcję Firewall powinien się integrować z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - a) Amazon Web Services (AWS).
 - b) Microsoft Azure.
 - c) Cisco ACI.
 - d) Google Cloud Platform (GCP).
 - e) OpenStack.
 - f) VMware NSX.
 - g) Kubernetes.

6.7 Połączenia VPN

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

6.8 Producent rozwiązania powinien posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klienckie VPN powinno być dostępne jako opcja i nie jest wymagane w implementacji.

6.9 Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- a) Routingu statycznego.
- b) Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
- c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
- d) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
- e) ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
- f) BFD (Bidirectional Forwarding Detection).
- g) Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

6.10 Funkcje SD-WAN

6.10.1 System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

6.10.2 SD-WAN powinien wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).

6.11 Zarządzanie pasmem

6.11.1 System Firewall powinien umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

6.11.2 System powinien dawać możliwość określania pasma dla poszczególnych aplikacji.

6.11.3 System powinien pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.

6.11.4 System powinien zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL

6.12 Ochrona przed malware

6.12.1 Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

6.12.2 Silnik antywirusowy powinien zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

6.12.3 W przypadku archiwów zagnieżdżonych powinna istnieć możliwość określenia, ile zagnieżdżeń kompresji system powinien próbować zdekompresować w celu przeskanowania zawartości lub umożliwiać konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

6.12.4 System powinien umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

6.12.5 System powinien dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

6.12.6 Baza sygnatur powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

6.12.7 System powinien współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz

z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.

- 6.12.8 Powinna istnieć możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.
- 6.12.9 Powinna istnieć możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

6.13 Ochrona przed atakami

- 6.13.1 Ochrona IPS powinna się opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- 6.13.2 System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- 6.13.3 Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 6.13.4 Administrator systemu powinien posiadać możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- 6.13.5 System powinien zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- 6.13.6 System powinien dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
- 6.13.7 Mechanizmy ochrony dla aplikacji Web'owych powinny być na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
- 6.13.8 Powinno być realizowane wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- 6.13.9 Powinna istnieć możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

6.14 Kontrola aplikacji

- 6.14.1 Funkcja Kontroli Aplikacji powinna umożliwić kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- 6.14.2 Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 6.14.3 Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- 6.14.4 Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- 6.14.5 Administrator systemu powinien posiadać możliwość definiowania wyjątków oraz własnych sygnatur.
- 6.14.6 Powinna istnieć możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
- 6.14.7 System powinien dawać możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

6.15 Kontrola WWW

- 6.15.1 Moduł kontroli WWW powinien korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- 6.15.2 W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
- 6.15.3 Filtr WWW powinien dostarczać kategorii stron zabronionych prawem np.: Hazard.

- 6.15.4 Administrator powinien posiadać możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- 6.15.5 Filtr WWW powinien umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
- 6.15.6 Filtr WWW powinien dawać możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
- 6.15.7 Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
- 6.15.8 Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
- 6.15.9 System powinien pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

6.16 Uwierzytelnianie użytkowników w ramach sesji

- 6.15.1 System Firewall powinien umożliwić weryfikację tożsamości użytkowników za pomocą:
 - a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
- 6.15.2 System powinien dawać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
- 6.15.3 System powinien umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
- 6.15.4 Realizować uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

6.17 Zarządzanie

- 6.17.1 Elementy systemu bezpieczeństwa powinny mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
- 6.17.2 Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania powinna być realizowana z wykorzystaniem szyfrowanych protokołów.
- 6.17.3 Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
- 6.17.4 System powinien współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
- 6.17.5 System powinien dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- 6.17.6 Element systemu pełniący funkcję Firewall powinien posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- 6.17.7 Element systemu realizujący funkcję Firewall powinien umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
- 6.17.8 Powinna być dostępna możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
- 6.17.9 Powinna być dostępna możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

6.18 Logowanie

- 6.18.1 Elementy systemu bezpieczeństwa powinny realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
- 6.18.2 W ramach logowania element systemu pełniący funkcję Firewall powinien zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- 6.18.3 Logowanie powinno obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
- 6.18.4 Powinna być dostępna możliwość włączenia logowania per reguła w polityce firewall.
- 6.18.5 System powinien zapewniać możliwość logowania do serwera SYSLOG.
- 6.18.6 Przesyłanie SYSLOG do zewnętrznych systemów powinno być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

6.19 Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).

6.20 Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje (Subskrypcje) które zapewniają:

- 6.20.1 Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.
- 6.20.2 Ochronę systemów przemysłowych SCADA
- 6.20.3 Oferowane oprogramowanie, systemy bezpieczeństwa oraz funkcjonalności realizowane w modelu licencyjnym lub subskrypcyjnym muszą być dostarczone w sposób zgodny z modelem licencjonowania producenta oraz obowiązującymi przepisami prawa.
- 6.20.4 Licencje oraz subskrypcje muszą zapewniać Zamawiającemu możliwość legalnego, nieprzerwanego i zgodnego z przeznaczeniem użytkowania systemów przez 36 miesięcy.
- 6.20.5 Elementy o charakterze czasowym, w szczególności:
 - a) subskrypcje bezpieczeństwa,
 - b) wsparcie producenta,
 - c) aktualizacje sygnatur, baz danych, reguł i mechanizmów ochronnych,
 - d) usługi chmurowe producenta niezbędne do działania systemu, podlegają finansowaniu ze środków projektu wyłącznie w zakresie przypadającym na okres do dnia określonego przez grantodawcę jako okres kwalifikowalności rozliczenia projektu.
- 6.20.6 Część licencji o okresie obowiązywania dłuższym niż okres kwalifikowalności projektu:
 - a) Do kosztów kwalifikowanych projektu zaliczona zostanie wyłącznie część kosztu licencji lub subskrypcji proporcjonalnie przypadająca na okres do dnia określonego przez grantodawcę jako okres kwalifikowalności rozliczenia projektu.
 - b) pozostała część kosztu finansowana będzie ze środków własnych Zamawiającego.
- 6.20.7 Licencje i subskrypcje:
 - a) nie mogą być uzależnione od obowiązku zawarcia dodatkowych umów po zakończeniu projektu,

b) nie mogą powodować powstania zobowiązań finansowych po stronie projektu grantowego po dniu określonym przez grantodawcę jako okres kwalifikowalności rozliczenia projektu.

6.20.8 Dostarczone licencje muszą:

- a) pochodzić z oficjalnego kanału dystrybucyjnego producenta lub autoryzowanego partnera,
- b) być wolne od wad prawnych,
- c) umożliwiać Zamawiającemu pełne korzystanie z funkcjonalności systemów zgodnie z SOPZ.

6.20.9 Wsparcie producenta oraz subskrypcje realizowane po dniu 30.06.2026 r. nie stanowią kosztów kwalifikowanych projektu „Cyberbezpieczne Wodociągi” i mogą być kontynuowane wyłącznie na podstawie odrębnej umowy, zawartej na zasadach rynkowych.

6.21 Gwarancja

6.21.1 Oferowane urządzenia muszą być fabrycznie nowe i objęte standardową gwarancją producenta, wliczoną w cenę zakupu urządzenia.

6.21.2 Okres standardowej gwarancji producenta nie może być krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru końcowego.

6.21.3 Gwarancja producenta obejmuje w szczególności:

- a) usuwanie wad sprzętowych,
- b) naprawę lub wymianę uszkodzonych komponentów na nowe lub równoważne,
- c) dostęp do aktualizacji oprogramowania systemowego (firmware) niezbędnych do prawidłowego i bezpiecznego funkcjonowania urządzenia.

6.21.4 Gwarancja powinna być realizowana jest przez producenta lub autoryzowanego partnera serwisowego, w trybie:

- a) NBD (Next Business Day) lub
- b) on-site w siedzibie Zamawiającego – zgodnie ze standardowymi warunkami producenta.

6.21.5 Gwarancja producenta:

- a) stanowi integralny element urządzenia,
- b) nie jest usługą odrębną,
- c) nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi”.

6.21.6 Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej.

Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.

6.21.7 Realizacja gwarancji po dniu określonym przez grantodawcę jako okres kwalifikowalności rozliczenia projektu nie powoduje powstania zobowiązań finansowych po stronie projektu grantowego i odbywa się zgodnie z warunkami standardowej gwarancji producenta.

6.22 Rozszerzenie Licencji NGFW dla OT o system PAM:

6.22.1 Wymagania funkcjonalne dla systemu:

1. Zapewnienie wysokiego poziomu bezpieczeństwa danych i poufności informacji
2. Wsparcie dla szyfrowania danych w transmisji i przechowywaniu haseł i kluczy
3. Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia
4. System powinien posiadać Mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu
5. System PAM powinien posiadać przyjazny interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.
6. Integracja z technologią ZTNA (Zero Trust Network Access) oraz możliwość działania jako punkt wymuszania dla ZTNA
7. Powinna istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola powinna być realizowana co najmniej dla transferu plików poprzez web (Web SFTP, Web

8. Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. System powinien monitorować komendy wydawane przez operatora sesji.
9. System PAM powinien być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania
10. Rozwiązanie powinien być dostępne w formie zarówno urządzeń wirtualnych (*virtual appliance*), jak i sprzętowych. Dla wirtualizacji powinien być wspierany co najmniej hypervisor VMWare oraz KVM.
11. Działanie PAM powinien pozwalać na obsługę połączeń bezpośrednich jak i proxy.
12. Możliwość obsługi niestandardowych protokołów chociażby poprzez dedykowane wyzwalacze (*custom application launcher*)
13. Możliwość ostrzegania użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO.
14. System PAM w wersji wirtualnej powinien obsługiwać moduł vTPM (*Virtual Trusted Platform Module*) dla przechowywania kluczy prywatnych użytkowników.
15. PAM powinien obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking”. Wszystkie działania w tym trybie powinny być logowane celem możliwości przeprowadzenia audytu.
16. System powinien automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking)
17. Powinna być automatyczna zmiana hasła konta po poprawnym zalogowaniu
18. Powinno być wsparcie dla zaplanowanej zmiany haseł według harmonogramu
19. Powinna istnieć możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów
20. Powinno być ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora. W tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.
21. Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile
22. Powinien być zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS
23. Kontrola dostępu powinna być oparta na rolach (RBAC)
24. Kontrola uprawnień powinna być oparta na użytkownikach oraz grupach użytkowników
25. Kontrola profili dostępowych powinna być realizowana w formie polityk
26. Powinno być wsparcie dla Disaster Recovery
27. Użytkownik uprzywilejowany powinien mieć możliwość pracy co najmniej w następujących trybach:
 - a) Agentowy – dostępne wszystkie funkcjonalności. Agent powinien być dostępny bezpłatnie
 - b) Bezagentowo, za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta powinna umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji
 - c) Bezagentowo, za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń.

6.22.2 Uwierzytelnianie

1. Obsługa uwierzytelniania użytkowników powinna być oparta na certyfikatach
2. Powinna istnieć możliwość korzystania z lokalnej bazy danych użytkowników.
3. Powinna istnieć obsługa uwierzytelniania wieloskładnikowego opartego na SAML.
4. Obsługa OIDC (openID Connect), SAML.
5. Powinna istnieć obsługa wielu połączeń SAML SP.
6. Powinna być możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.
7. Powinno być wsparcie dla integracji z istniejącymi systemami zarządzania tożsamościami
8. Powinna być możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji
9. Dostęp do zasobów użytkowników uprzywilejowanych powinien również obejmować możliwości blokady w oparciu o dodatkowe parametry:
 - a) Kontrola dostępu oparta na adresie źródłowym IP użytkownika

- b) Ograniczanie dostępu oparte na harmonogramie użytkownika
- c) Kontrola dostępu do docelowego serwera oparta o przypisane tagi ZTNA (stan stacji, z której następuje połączenie jest badany przez mechanizmy ZTNA)

6.22.3 Licencjonowanie

1. Oprogramowanie powinno być objęte kompletną licencją producenta na całe rozwiązanie. Nie dopuszcza się dodatkowych wymagań licencyjnych dla systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych.
2. Nie dopuszcza się licencjonowania ilości zasobów, do których realizowany jest nadzorowany dostęp.
3. Nie dopuszcza się licencjonowania ilości zajętego miejsca na dysku przez nagrania sesji.
4. Licencja systemu powinna pozwalać na jednoczesne podłączenie się co najmniej 5 aktywnych użytkowników do monitorowanych zasobów. Licencja PAM musi zapewniać możliwość legalnego i nieprzerwanego korzystania z funkcjonalności PAM co najmniej przez 36 miesięcy.
5. Ponieważ model licencjonowania producentów przewiduje licencję o okresie obowiązywania dłuższym niż okres kwalifikowalności projektu:
 - a) Zamawiający dopuszcza dostarczenie licencji obejmującej okres wykraczający poza dzień określony przez grantodawcę jako okres kwalifikowalności rozliczenia projektu.
 - b) do kosztów kwalifikowanych projektu zaliczona zostanie wyłącznie część kosztu licencji proporcjonalnie przypadająca na okres do dnia 30.06.2026 r.,
 - c) pozostała część kosztu licencji finansowana będzie ze środków własnych Zamawiającego.
6. Licencja PAM:
 - a) musi pochodzić z oficjalnego kanału dystrybucyjnego producenta lub autoryzowanego partnera,
 - b) musi być wolna od wad prawnych,
 - c) nie może być uzależniona od obowiązku zawarcia dodatkowych umów po zakończeniu projektu.
7. Wsparcie producenta oraz subskrypcje związane z licencją PAM realizowane po dniu 30.06.2026 r. nie stanowią kosztów kwalifikowanych projektu „Cyberbezpieczne Wodociągi” i mogą być kontynuowane wyłącznie na podstawie odrębnej umowy, zawartej na zasadach rynkowych.
8. Licencja powinna pozwalać na użytkowanie rozwiązania co najmniej w okresie obowiązywania zakontraktowanej gwarancji wsparcia technicznego.

6.22.4 Monitorowanie i raportowanie

1. Powinna istnieć możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi.
2. Powinna być możliwość generowania szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników

6.22.5 Gwarancja i wsparcie techniczne

1. Oferowane rozszerzenie licencji NGFW dla OT o system PAM musi być objęte gwarancją producenta oraz wsparciem technicznym producenta lub autoryzowanego partnera producenta.
2. Gwarancja oraz wsparcie techniczne obejmują:
 - a) dostęp do aktualizacji oprogramowania systemu PAM,
 - b) dostęp do poprawek bezpieczeństwa (security fixes),
 - c) usuwanie błędów systemowych i nieprawidłowości działania wynikających z wad oprogramowania,
 - d) dostęp do pomocy technicznej producenta lub autoryzowanego partnera.
3. Wsparcie techniczne powinno być świadczone w trybie minimum 8x5, z możliwością eskalacji zgłoszeń krytycznych. Zamawiający dopuszcza świadczenie wsparcia w trybie 24x7, o ile stanowi ono standard producenta i nie powoduje zwiększenia ceny oferty.
4. Okres gwarancji i wsparcia technicznego musi obejmować co najmniej 36 miesięcy. Do kosztów kwalifikowanych projektu zaliczona zostanie wyłącznie część kosztu przypadająca na okres do dnia określonego przez grantodawcę jako termin kwalifikowalności projektu. Realizacja świadczeń po tym dniu zostanie sfinansowana ze środków własnych zamawiającego i nie może powodować powstania dodatkowych zobowiązań finansowych po stronie projektu.

5. Gwarancja i wsparcie techniczne nie mogą być uzależnione od obowiązku zawarcia po dniu określonym przez grantodawcę jako termin kwalifikowalności projektu dodatkowych umów serwisowych, subskrypcyjnych lub utrzymaniowych.
6. Po zakończeniu okresu finansowania projektu Zamawiający dopuszcza możliwość kontynuacji wsparcia systemu PAM na podstawie odrębnej umowy, zawartej na zasadach rynkowych.

7. Switch zarządalny dla OT – 3 szt.

7.1 Przełącznik sieciowy

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu powinny zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

7.2 Parametry fizyczne urządzenia

- a) Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- b) Zasilanie AC 230V.
- c) Maksymalny pobór mocy: 10 W.
- d) Minimalny zakres temperatury pracy: 0-40°C.
- e)

7.3 Interfejsy sieciowe - wymagania minimalne

Wymagany jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

- a) 8 porty GE RJ-45.
- d) 2 porty GE, SFP.

7.4 Zarządzanie

Urządzenie powinno posiadać:

- a) Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- b) Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- c) Wsparcie dla SNMP w wersjach 1-3
- d) Funkcję zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- e) Funkcję aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- f) Konfigurację w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- g) Funkcję backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- h) Funkcję definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- i) Funkcję definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- j) Automatyczne wykonywanie rewizji konfiguracji.

7.5 Parametry wydajnościowe

- a) Wymagana przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
- b) Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
- c) Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.

7.6 Wymagane funkcje

- a) Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- b) Obsługa Jumbo Frames.
- c) Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- d) Agregacja portów zgodna ze standardem 802.3ad.
- e) Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- f) Obsługa routingu statycznego.
- g) Port-mirroring.
- h) Uwierzytelnianie 802.1x na poziomie portu.
- i) Uwierzytelnianie 802.1x w oparciu o adres MAC.
- j) W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- k) W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- l) W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

7.7 Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

- 7.7.1 Przełączniki powinny wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf).
- 7.7.2 Zakres zarządzania przez element nadrzędny powinien zawierać co najmniej:
 - a) Centralne zarządzanie konfiguracją urządzenia
 - b) Aktualizację oprogramowania realizowaną z systemu centralnego zarządzania
 - c) Centralne zarządzanie sieciami VLAN.
 - d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
 - f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - g) Integrację z systemem kontroli dostępu. Urządzenie powinno podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - h) Automatyczną detekcję i rekomendacje konfiguracji.
 - i) Przesyłanie logów na zewnętrzny serwer syslog.
 - j) Funkcję uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - k) Obsługę białych i czarnych list adresów MAC.
 - l) Wykrywanie aplikacji komunikujących się w sieci.
- 7.7.3 Powinno być możliwe redundantne połączenie z elementami zarządzającymi.
- 7.7.4 W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

7.8 Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- 7.8.1 System powinien realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- 7.8.2 System powinien zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

7.9 Gwarancja

- 1) Oferowane switche zarządzalne muszą być fabrycznie nowe i objęte standardową gwarancją producenta, wliczoną w cenę zakupu urządzenia.
- 2) Okres standardowej gwarancji producenta na switchy nie może być krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru końcowego.
- 3) Gwarancja producenta obejmuje w szczególności:
 - a) usuwanie wad sprzętowych,
 - b) naprawę lub wymianę uszkodzonych komponentów na nowe lub równoważne,
 - c) dostęp do aktualizacji oprogramowania systemowego (firmware) niezbędnych do prawidłowego i bezpiecznego funkcjonowania urządzenia.
- 4) Gwarancja powinna być realizowana jest przez producenta lub autoryzowanego partnera serwisowego, w trybie:
 - a) NBD (Next Business Day) lub
 - b) on-site w siedzibie Zamawiającego – zgodnie ze standardowymi warunkami producenta.
- 5) Gwarancja producenta:
 - a) stanowi integralny element urządzenia,
 - b) nie jest usługą odrębną,
 - c) nie stanowi odrębnego kosztu kwalifikowanego projektu „Cyberbezpieczne Wodociągi”.
- 6) Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej.
Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
- 8) W powyższym przypadku okres gwarancji musi wciąż obejmować co najmniej 36 miesięcy. Do kosztów kwalifikowanych projektu zaliczona zostanie wyłącznie część kosztu przypadająca na okres do dnia określonego przez grantodawcę jako termin kwalifikowalności projektu. Realizacja świadczeń po dniu określonym przez grantodawcę jako termin kwalifikowalności projektu zostanie sfinansowana ze środków własnych zamawiającego i nie może powodować powstania dodatkowych zobowiązań finansowych po stronie projektu.

8.Szafa RACK do systemów bezpieczeństwa – 2 szt.

Parametry minimalne
Wymiary podstawowe: 19"/15U
Wysokość max. [mm] 769
Szerokość max. [mm] 600
Głębokość max. [mm] 600
Tył: zamknięty, możliwość otwarcia
Otwierany bok
Ilość szyn rack: 4
Regulacja szyn rack w pełnym zakresie
Możliwość zamontowania wentylatorów
Waga max [kg] 26
Nośność minimalna [kg]: 80

Normy wykonania: Zgodność z normami ANSI/EIA RS-310-D, DIN41491 PART1, IEC297-2, DIN41494 PART7, GB/T3047.2-92

Kompatybilność ze standardami: metrycznym ETSI oraz międzynarodowym 19".

Szafy powinny być wyposażone w panel wentylacyjny 19" LCD 1U 230 VAC z dwoma wentylatorami i termostatem.

Gwarancja na urządzenie:

1. Oferowana szafa RACK do systemów bezpieczeństwa musi być objęta standardową gwarancją producenta, wliczoną w cenę dostawy.
2. Okres gwarancji producenta nie może być krótszy niż 24 miesiące, liczony od dnia podpisania protokołu odbioru końcowego.
3. Gwarancja producenta obejmuje w szczególności:
 - a) wady materiałowe i produkcyjne konstrukcji szafy,
 - b) stabilność i nośność konstrukcji zgodnie z parametrami określonymi w OPZ,
 - c) poprawność działania elementów mechanicznych, w tym drzwi, zamków, zawiasów, prowadnic i szyn montażowych,
 - d) trwałość powłok lakierniczych oraz odporność na korozję w warunkach eksploatacji zgodnych z przeznaczeniem,
 - e) kompletność dostarczonych elementów wyposażenia.
4. Gwarancja nie obejmuje uszkodzeń mechanicznych powstałych w wyniku:
 - a) niewłaściwego użytkowania,
 - b) przeciążenia szafy ponad dopuszczalne wartości,
 - c) ingerencji osób trzecich nieuprawnionych przez Zamawiającego.
5. Gwarancja powinna być realizowana jest w formie naprawy lub wymiany wadliwych elementów konstrukcyjnych na wolne od wad, bez dodatkowych kosztów po stronie Zamawiającego.
6. Gwarancja producenta jako element wliczony w cenę szafy RACK, nie stanowi odrębnego kosztu kwalifikowanego projektu.
7. Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej. Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
8. Zamawiający nie dopuszcza wyodrębniania w ofercie pozycji kosztowych dotyczących gwarancji lub świadczeń realizowanych po dniu określonym przez grantodawcę jako termin kwalifikowalności projektu.

9. UPS do systemów cyberbezpieczeństwa – 1 szt.

PARAMETR	WARTOŚĆ MINIMALNA
Napięcie wejściowe	230 V AC, 1 faza
Maksymalna konfigurowalna moc (W)	2700W
Maksymalna konfigurowalna moc (VA)	3000 VA
Liczba gniazd wyjściowych	6 × IEC 320 C13 + 1 × IEC 320 C19,
Częstotliwość sieciowa	50/60 Hz ±3 Hz, automatyczne wykrywanie
Napięcie wyjściowe	230 V AC, 1 faza
Typ przebiegu	Sinusoida

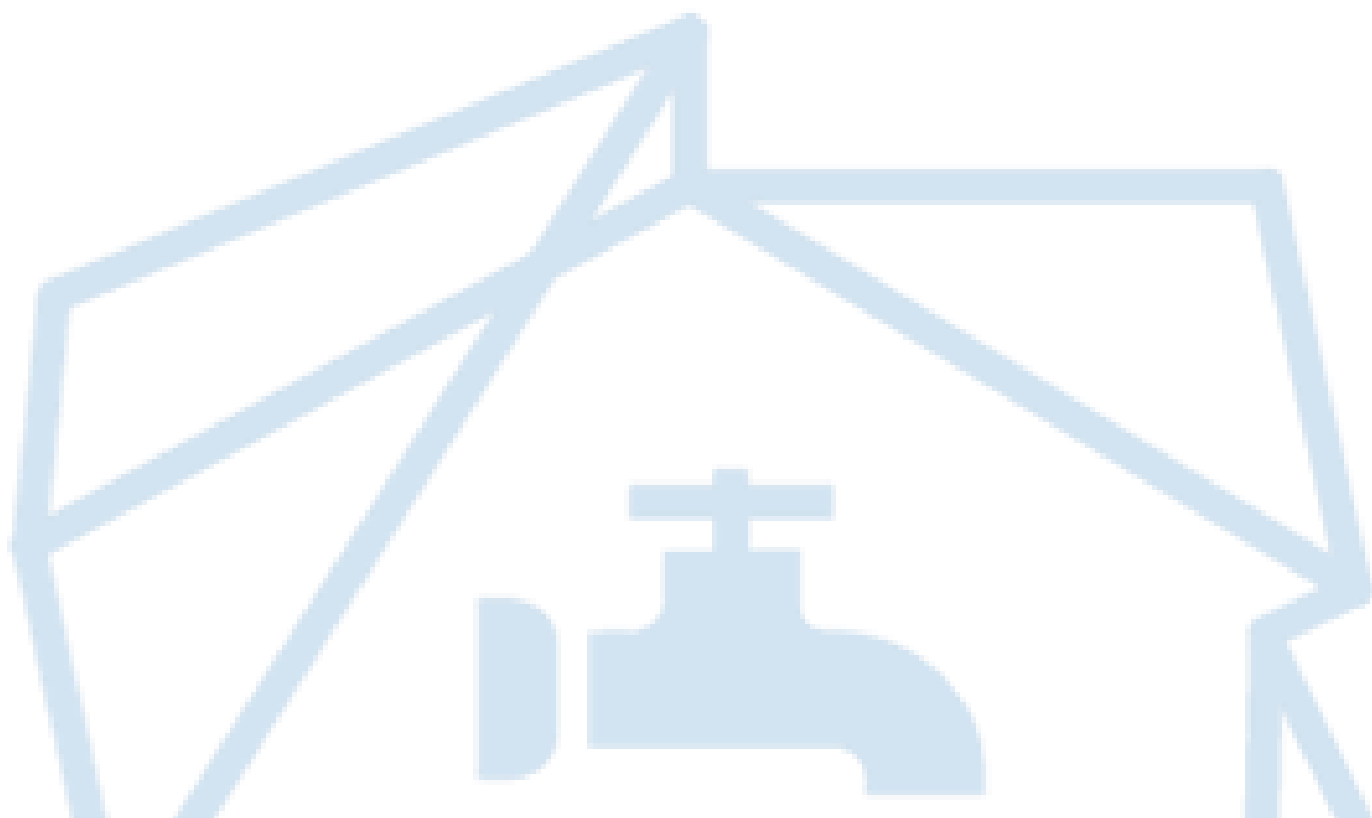
PARAMETR	WARTOŚĆ MINIMALNA
Współczynnik mocy wejściowej	> 0,99
Rozdział zniekształcenia napięcia wyjściowego. (obciążenie liniowe) — maks.	< 3 %
Typ baterii	Wewnętrzna szczelna.
Parametry znamionowe akumulatora	12 V / 9 Ah
Wymiana akumulatorów	Wymienne baterie
Zarządzanie akumulatorem	Metoda ładowania z kompensacją temperaturową. Automatyczny test baterii. Ochrona przed głębokim rozładowaniem.
Awaryjny wyłącznik zasilania	Tak
Panel przedni	Wielofunkcyjny wyświetlacz LCD
Interfejsy komunikacyjne	Port USB (HID), Port szeregowy (RS232), Mini-blok zacisków do zdalnego wyłączenia
Karta sieciowa	Pre-instalowana
Format rack	Maks 2U
Sposób montażu	Zestaw w komplecie: Zestaw do montażu w szafie rack powinien zawierać (szyny i uchwyty). Instrukcje dotyczące bezpieczeństwa, Szybki start
Alarmy	Praca na baterii, niski poziom baterii, przeciążenie (dźwiękowe)
Format rack	Maks 2U
Masa	Max 35 kg
Kompatybilność USB	Tak
Wyposażenie	CD z oprogramowaniem, dokumentacja, instrukcja montażu, szyny rack, nóżki, kabel RS-232, kabel USB
Normy	EN/IEC 62040-1:2019/A11:2021; EN/IEC 62040-2:2006/AC:2006; EN/IEC 62040-2:2018
Temperatura pracy	0...45 °C
Temperatura przechowywania	-15...45 °C
Poziom hałasu	Max 40 dBA

Gwarancja na urządzenie:

- 1) Oferowany zasilacz awaryjny UPS musi być objęty standardową gwarancją producenta, wliczoną w cenę urządzenia.
- 2) Okres gwarancji producenta nie może być krótszy niż 36 miesięcy dla urządzenia i 24 miesiące dla akumulatorów, liczony od dnia podpisania protokołu odbioru końcowego.
- 3) Gwarancja producenta obejmuje w szczególności:
 - a) wady fabryczne urządzenia,
 - b) awarie elektroniki, toru mocy oraz układów sterujących,
 - c) prawidłowe działanie układów zabezpieczeń,
 - d) poprawność pracy systemu zarządzania i komunikacji (w tym karty sieciowej),
 - e) zgodność parametrów technicznych z deklaracją producenta.
- 4) Zamawiający wymaga, aby gwarancja realizowana była w trybie serwisu producenta lub autoryzowanego serwisu producenta, z zapewnieniem naprawy lub wymiany urządzenia na wolne od wad.
- 5) W przypadku braku możliwości naprawy UPS w rozsądnym terminie (21 dni), producent lub autoryzowany serwis zobowiązany jest do wymiany urządzenia na nowe lub równoważne, o parametrach nie gorszych

niż wymagane w SOPZ lub zapewnić urządzenie zastępcze na czas naprawy o porównywalnych parametrach.

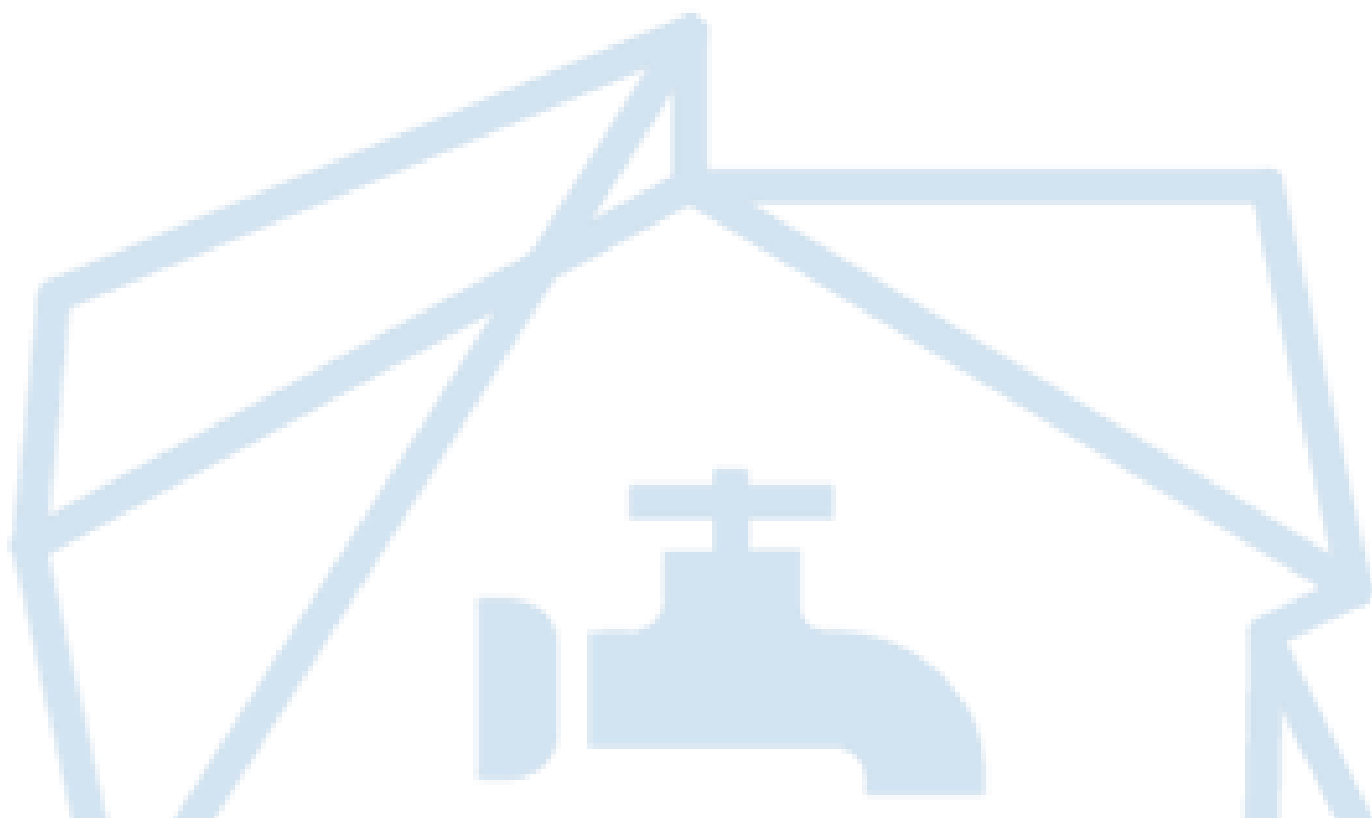
- 6) Gwarancja producenta jako element wliczony w cenę urządzenia, nie stanowi odrębnego kosztu kwalifikowanego projektu.
- 7) W przypadku, gdy producent oferuje standardowo dłuższy okres gwarancji:
 - a) Zamawiający dopuszcza objęcie UPS gwarancją wykraczającą poza dzień określony przez grantodawcę jako termin kwalifikowalności projektu,
 - b) do kosztów kwalifikowanych projektu zaliczona zostanie wyłącznie część kosztu przypadająca na okres do dnia określonego przez grantodawcę jako termin kwalifikowalności projektu ,
 - c) realizacja świadczeń po dniu po dniu określonym przez grantodawcę jako termin kwalifikowalności projektu. nie może powodować powstania dodatkowych zobowiązań finansowych po stronie projektu grantowego.
- 8) Jeżeli gwarancja jest standardowym elementem urządzenia – nie wyodrębnia się jej.
Jeżeli producent technicznie wymusza osobną pozycję, Zamawiający dopuszcza jej wykazanie informacyjnie, bez wpływu na cenę kwalifikowaną.
- 9) W przypadku, gdy producent przewiduje inny okres gwarancji na akumulatory niż na całe urządzenie UPS:
 - a) okres gwarancji na akumulatory nie może być krótszy niż 24 miesiące,
 - b) warunki gwarancji na akumulatory muszą być zgodne z dokumentacją producenta,
 - c) gwarancja na akumulatory nie stanowi odrębnego kosztu kwalifikowanego projektu.



Zadanie 2

Spis treści.

1.PLATFORMA SIEM (MONITOROWANIE , PODATNOSCI,INWENTARYZACJA ,CTI).....	45
2. OPROGRAMOWANIE TYPU EDR/XDR DO INTEGRACJI Z SIEM.....	63



1. Platforma SIEM (monitorowanie, podatności, inwentaryzacja, CTI)

LICENCJA

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

Oprogramowanie powinno posiadać wsparcie do dnia określonego jako data końcowa kwalifikowalności wydatków finansowanych w ramach udzielonego grantu (warunek konieczny z uwagi na finansowanie z grantu), w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

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

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

WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej zwany CSB) powinien używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.

Monitorowanie Wysokiej Wydajności: CSB powinno umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB powinno efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien posiadać skalowalną architekturę dostosowaną do ilości urządzeń obsługiwanych w infrastrukturze Zamawiającego w ilości minimum **90 urządzeń końcowych**.

Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie powinna być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.

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

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

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

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

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

Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów powinien być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.

Szybkość i Wydajność: CSB powinien być zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

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

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

Odkrywanie i Analiza Danych: CSB powinien umożliwiać użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

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

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

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

Na podstawie uzyskanych efektów serwis powinien posiadać możliwość udostępnienia publicznego.

Treści multimedialne powinny 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.

Powinna być zachowana zgodność ze standardami HTML i CSS całego serwisu www.

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

System CSB powinien rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

Centralny System Bezpieczeństwa **powinien posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system powinien posiadać co najmniej moduły:**

1. MODUŁ ANALIZY PODATNOŚCI

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

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

Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki powinna odbywać się przynajmniej raz dziennie. Po zalogowaniu do systemu 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 innym kolorem.

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

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

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

CSB powinien informować użytkownika/administradora o nowych podatnościach występujących w infrastrukturze sieciowej **Zamawiającego**. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administradora 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. CSB musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

2. MODUŁ MONITORINGU ZASOBÓW

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

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

2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami.

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

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

CSB powinien 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-maili lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskazać zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi

mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

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

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

2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej.

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

2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT.

CSB powinien 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 wskazać zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT.

CSB powinien 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 wskazać zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.8 Zdalny dostęp do urządzeń końcowych.

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

2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych.

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

2.10 Analiza ruchu sieciowego.

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

2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach.

CSB powinien 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.

3. MODUŁ ANALIZY LOGÓW

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

Moduł Analizy Logów i Moduł Monitoringu Zasobów powinien 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 CBS musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzicznych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

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

CBS powinien 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 systemem.

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

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

3.4. Przegląd i analiza logów dotyczących działań użytkowników.

W module analizy logów powinien 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 poprzez wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

3.5. Dostęp do logów historycznych.

CBS oprócz dostępu do aktualnych logów powinien 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 poczynawszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

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

CBS powinien 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 kątem istotności pojawiającego się wpisu w logach oraz wyboru typu logu (m.in. log systemowy, log „customowy”). Ponadto CSB musi informować użytkownika/administratora o „nowych” zagregowanych logach z poszczególnego hosta. Informacja ta

powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a “nowe” logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

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

CBS powinien 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).

4. MODUŁ EDR/XDR

4.1 CBS powinien 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.

4.2 Moduł powinien posiadać podgląd informacji, alertów i zdarzeń- występujących w środowisku IT. W CSB powinna być możliwość podglądu statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

4.3 Oprócz posiadanego modułu EDR/XDR, system powinien 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.

5. MODUŁ INWENTARYZACJI

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

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

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

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

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

Moduł powinien być wyposażony w funkcjonalności umożliwiające użytkownikowi/administratorowi wygenerowanie 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 informacje 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.

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

6.1. Integracja z systemem tiketowym.

System CSB powinien 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 zawierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

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

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

6.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

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

7. MODUŁ WYKRYWANIA ZAGROŻEŃ

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

System powinien 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 macierzy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System powinno 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 macierzy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

7.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń.

CSB powinien umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia muszą 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.

7.3. Historia wykrytych zagrożeń.

CSB powinien 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).

7.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia.

CSB powinien 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 wykonana 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.

8. MODUŁ RAPORTÓW

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

CSB powinien posiadać możliwość tworzenia 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 musi mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

9. PANEL UŻYTKOWNIKA

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

Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora systemu 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.

9.2. Wizualizacja statystyk zdarzeń i logów.

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

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

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

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

Panel użytkownika CSB 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 umożliwiającą 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.

9.5. Intuicyjny panel zarządzania regułami i definiowania "customowych" logów.

Panel użytkownika CSB 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.

10. MODUŁ ANALIZY DANYCH AI

System CSB powinien 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.

10.1 Analiza bieżących logów.

Moduł powinien umożliwić 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.

10.2 Analiza wykrytych zagrożeń.

Moduł powinien 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

10.3 Analiza problemów.

Moduł powinien umożliwić użytkownikowi uruchomienie asystenta AI w celu przeanalizowania problemów występujących na poszczególnych hostach zareportowanych 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.

11. MODUŁ THREAT INTELLIGENCE

System CSB powinien 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.

11.1 Lista wskaźników – MALWARE.

Lista wskaźników dotyczących złośliwego oprogramowania musi zawierać istotne informacje na temat zgłoszonego zdarzenia. Na liście tej powinny znaleźć się co najmniej informacje 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 zainfekowanego 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.

11.2 Lista wskaźników – zagrożenia sieciowe.

Lista wskaźników dotyczących zagrożeń sieciowych powinna zawierać istotne informacje na temat zgłoszonego zdarzenia. Lista ta musi zawierać co najmniej informacje 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 poziomu modułu do źródła zawierającego więcej szczegółowych informacji.

11.3 Lista wskaźników – złośliwe adresy URL.

Lista wskaźników dotyczących złośliwych adresów URL powinna zawierać istotne informacje na temat zgłoszonych zdarzeń. Lista ta musi zawierać informacje 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 poziomu modułu do źródła zawierającego więcej szczegółowych informacji.

11.4 Lista blokowanych plików.

Moduł powinien umożliwiać użytkownikowi wyświetlenie listy plików przez niego zablokowanych na liście wskaźników typu malware. Umieszczone na tej liście pliki muszą być wykrywane przez agentów systemu i blokowane w celu ochrony poszczególnych hostów. Użytkownik powinien mieć również możliwość ręcznego dodawania plików do tej listy poprzez podanie formatu 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 i IOS.

11.5 Wyszukiwanie i filtrowanie.

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

12. MODUŁ UEBA

System CSB powinien 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.

12.1 Predefiniowane reguły wykrywania anomalii UEBA.

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

- podejrzanej aktywności systemów, reguła musi analizować zdarzenia systemowe, takie jak zmiany w rejestrze, zmiany czasu systemowego, zmiany w konfiguracji rozruchu czy instalacje aktualizacji, w celu wykrycia nietypowych działań mogących sugerować próbę manipulacji lub nieautoryzowanego dostępu do systemu,
- zapytań DNS do podejrzanych lokalizacji geograficznych, reguła musi analizować zapytania do serwerów DNS znajdujących się w nietypowych krajach w stosunku do standardowego ruchu organizacji, mogących wskazywać na działania związane z malwarem lub wyciekiem danych,
- potencjalnego zachowania użytkowników wskazujące na atak typu DDoS, reguła musi umożliwiać detekcję nietypowej intensywności aktywności użytkownika, mogącej sugerować atak rozproszony typu (DDoS) lub infekcję systemu,
- nietypowych zachowań użytkowników w zdarzeniach bezpieczeństwa, reguła musi analizować nietypowe wzorce aktywności użytkowników, takie jak nagły wzrost liczby zdarzeń bezpieczeństwa lub działania poza standardowymi godzinami pracy,
- podejrzanych logowań lub eskalacji uprawnień, reguła musi wykrywać anomalie, w zachowaniach takich jak logowania z nieznanych lokalizacji lub kont o wysokich uprawnieniach

12.2 Parametryzacja i trenowanie zaimplementowanych modeli ML.

System CSB powinien dawać możliwość trenowania zaimplementowanych modeli ML oraz ich automatyczne douczanie. W systemie musi być możliwość wybrania detektora dla wybranej reguły UEBA i podglądu 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 informacje 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.

12.3 Prezentacja i wizualizacja wykrytych anomalii.

System CSB powinien 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

12.4 Wektor ataku.

System powinien 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.

12.5 Wyszukiwanie i filtrowanie.

Moduł powinien 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.

13. MODUŁ OBSŁUGI ZGŁOSZEŃ

13.1 System CSB powinien 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 naruszenia bezpieczeństwa. Formularz zgłoszeniowy musi zawierać następujące pola: imię i nazwisko, adres e-mail, temat, wiadomość. Wysyłanie zgłoszeń musi być zabezpieczone mechanizmem reCAPTCHA.

13.2 Moduł obsługi zgłoszeń powinien 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.

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

14. MODUŁ SYMULACJI ATAKU

System CSB powinien być wyposażony w moduł symulacji ataku umożliwiający sprawdzenie zabezpieczeń wprowadzonych przez Zamawiającego. 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 przeszukującą po polach dostępnych dla listy agentów, Scenariuszy oraz utworzonych i wykonanych symulacji.

14.1 Scenariusze ataków.

System CSB powinien być wyposażony w co najmniej 25 różnych scenariuszy umożliwiających testowanie zabezpieczeń. Scenariusze te powinny testować możliwości takie jak min: Screen Capture, Copy Clipboard, Get Chrome Bookmarks, Record microphone, Create staging directory, Find files, Stage sensitive files, Compress staged directory, Exfil staged directory, Discover Antivirus programs, Scan WIFI networks, Sniff network traffic, Add bookmark, Avoid logs, Disable Windows Defender All, Move Powershell & trace, Clear Logs, Advanced File Search and Stager, Compress staged directory, Exfil Compressed Archive to FTP Server, WMIC Process Enumeration, tasklist Process Enumeration, PowerShell Process Enumeration, UAC Status, SysInternals PSToll Process Discovery, Identify active user, Collect ARP details, Identify system processes, Preferred WIFI, Disrupt WIFI, Reverse 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, Leverage Procdump for Isass memory, Signed Binary Execution – odbccnf, Signed Binary Execution – Mavinject oraz wiele innych. Wybór predefiniowanego scenariusza musi odbywać się z poziomu UI systemu.

14.2 Symulacje ataków.

System CSB powinien 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 informacja na temat jej przebiegu na dodanych agentach. Po wyświetleniu szczegółów przebiegu symulacji w systemie muszą znajdować się informacje takie jak: Data rozpoczęcia symulacji, nazwa wykonywanej operacji (np. Current User) nazwa taktyki/techniki z MITRE (np. discovery T1033 – 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).

15. MODUŁ SLA

System CSB powinien 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.

15.1 Ustawienia SLA.

System CSB powinien 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.

15.2 Lista zdarzeń dla podatności CVE.

Moduł SLA powinien 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 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 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.

15.3 Lista zdarzeń dla problemów.

Moduł SLA powinien 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.

15.4 Lista zdarzeń dla zagrożeń.

Moduł SLA powinien 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.

15.5 Lista Incydentów EDR.

Moduł SLA powinien 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 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 incydentu, którego to zdarzenie dotyczy, przypisania operatora, który jest odpowiedzialny za tego typu zdarzenie, przypisania

zdarzenia do powiązanego zdarzenia w celu ich zgrupowania oraz reakcji na dane zdarzenie, przy każdym zmianie statusu zdarzenia użytkownik musi mieć możliwość pozostawienia notatki dotyczącej jego obsługi. Lista zdarzeń dotyczących incydentów EDR musi umożliwiać przeglądnięcie historii obsługi zdarzenia wraz ze wskazaniem zmiany statusu notatki oraz operatora, który zajął się obsługą.

1.2. Wdrożenie platformy SIEM

Wykonawca zrealizuje wdrożenie systemu SIEM w uzgodnionym z Zamawiającym terminie, w formule umożliwiającej realizację prac zdalnie, o ile warunki techniczne i bezpieczeństwa po stronie Zamawiającego na to pozwolą (w szczególności zapewnienie zdalnego dostępu dla Wykonawcy zgodnie z obowiązującymi u Zamawiającego zasadami). Przed rozpoczęciem prac wdrożeniowych Zamawiający przygotuje niezbędne elementy do wdrożenia, w tym w szczególności: infrastrukturę/środowisko (serwer/VM lub zasoby chmurowe – zgodnie z przyjętym modelem wdrożenia), dostęp sieciowy pomiędzy komponentami, konta i uprawnienia administracyjne wymagane do instalacji i konfiguracji, a także listę źródeł logów/danych przewidzianych do podłączenia wraz z informacją o sposobie ich udostępnienia (np. syslog/WEF/API) oraz osoby kontaktowe po stronie Zamawiającego odpowiedzialne za udostępnienie dostępu i wsparcie integracji. Wykonawca musi spełnić wszystkie ww. wymagania Zamawiającemu, niezbędne do prawidłowego przeprowadzenia wdrożenia min. 14 dni przed planowanym wdrożeniem.

- a) dostarczyć licencję systemu SIEM (wraz z wymaganymi modułami),
- b) dostarczyć lub udostępnić niezbędne komponenty sprzętowe lub wirtualne,
- c) zapewnić kompatybilność rozwiązania z infrastrukturą Zamawiającego,
- d) dostarczyć oprogramowanie w wersji aktualnej i wspieranej przez producenta.

W ramach wdrożenia Wykonawca przeprowadzi instalację i konfigurację systemu SIEM, podłączy uzgodnione źródła danych oraz skonfiguruje podstawowe elementy działania systemu w zakresie wymaganym OPZ (w tym co najmniej: odbiór i prezentację danych, wyszukiwanie, alertowanie oraz niezbędne dashboards/raporty wynikające z podłączonych źródeł). Po zakończeniu konfiguracji Wykonawca przygotuje i przeprowadzi wspólnie z Zamawiającym testy działania obejmujące weryfikację poprawności zbierania danych ze wskazanych źródeł, podstawowej poprawności przetwarzania oraz działania skonfigurowanych mechanizmów alertowania i prezentacji; scenariusze testowe zostaną uzgodnione z Zamawiającym i będą stanowiły podstawę odbioru wdrożenia.

Wykonawca przeprowadzi szkolenie zdalne dla wskazanych przez Zamawiającego osób (3 osób) w zakresie niezbędnym do bieżącej obsługi i podstawowej administracji systemem, w języku polskim, wraz z przekazaniem materiałów szkoleniowych.

Po odbiorze wdrożenia Wykonawca zapewni dodatkowe wsparcie powdrożeniowe przez okres do 30.06.2026 r., realizowane zdalnie, obejmujące konsultacje oraz wprowadzanie uzgodnionych korekt konfiguracyjnych wynikających z eksploatacji rozwiązania w środowisku Zamawiającego (w szczególności w zakresie działania integracji oraz konfiguracji elementów, które były przedmiotem wdrożenia).

2. Oprogramowanie typu EDR/XDR do integracji z SIEM

<p>LICENCJA</p>	<p>W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Licencja powinna mieć charakter czasowy i obowiązywać przez okres 12 miesięcy od daty wdrożenia. Do dofinansowania zgłoszona została wyłącznie część kosztu licencji proporcjonalnie przypadająca na okres kwalifikowalności projektu, tj. od wdrożenia do 30.06.2026 r. Pozostała część kosztu licencji zostanie sfinansowana ze środków własnych Zamawiającego (beneficjenta)</p> <p>Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. 12 miesięczną gwarancję producenta dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).</p> <p>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.</p> <p>Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.</p> <p>Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.</p> <p>Przedmiotem zamówienia będzie dostarczenie następujących ilości licencji:</p> <ul style="list-style-type: none"> - Serwerowe – 7 szt. docelowo 9 w tym (do 20 maszyn wirtualnych) - Komputerowe – 90 szt. - Urządzenia mobilne – 25 szt.
<p>Ochrona punktów końcowych urządzeń komputerowych</p>	<p>Ochrona antywirusowa niżej wymienionego systemu powinna być monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.</p> <p>Od strony chronionego środowiska nie powinna być 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.</p> <p>Ten sam agent zainstalowany na systemach Windows powinien umożliwiać rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji powinna być uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymagać reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.</p> <p>Rozwiązanie dla ochrony antywirusowej stacji roboczych powinno wspierać następujące systemy operacyjne:</p> <ul style="list-style-type: none"> • Microsoft Windows 10 • Microsoft Windows 11 • macOS 15 "Sequoia" • macOS 14 "Sonoma"

	<ul style="list-style-type: none"> • macOS 13 "Ventura" <p>Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:</p> <ul style="list-style-type: none"> • Microsoft Edge • Mozilla Firefox • Google Chrome • Safari <p>Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych powinno posiadać Polski interfejs użytkownika.</p> <p>Ten sam agent zainstalowany na systemach Windows powinien umożliwiać 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.</p> <p>Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy powinny być zarządzane z tej samej konsoli zarządzającej</p> <ol style="list-style-type: none"> 1. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, powinno mieć możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku. 2. Agent instalowany na stacjach końcowych powinien posiadać możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory. 3. Agent instalowany na stacjach końcowych powinien posiadać możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 4. Oprogramowanie nie powinno wymagać restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych. 5. Dane zebrane przez agenta instalowanego na stacjach końcowych powinny być przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 6. Agent instalowany na stacjach końcowych powinien monitorować i zbierać informacje na temat co najmniej następujących zdarzeń: <ul style="list-style-type: none"> • dostęp do pliku; • tworzenie nowego procesu; • nawiązane połączenia sieciowe; • wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa; • zawartość skryptów uruchamianych na monitorowanej stacji. 7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń powinny
--	--

	<p>odbywać się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.</p> <ol style="list-style-type: none"> 8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, powinny być kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, powinna odbywać się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 10. Komunikacja agentów instalowanych na stacjach roboczych, powinna wspierać komunikację za pomocą serwera pośredniczącego http (http proxy). 11. 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 powinny być buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 12. Dane zbierane przez agentów na stacjach końcowych powinny być przechowywane i przetwarzane na obszarze Unii Europejskiej. 13. Rozwiązanie na bazie zebranych danych powinny generować detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych. 14. Detekcje powinny być generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 15. Detekcje powinny być generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym. 16. Detekcje powinny być widoczne w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 17. Detale dotyczące detekcji powinny być przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. 18. Rozwiązanie powinno posiadać możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 19. Każda detekcja powinna zawierać co najmniej następujące informacje: <ul style="list-style-type: none"> • 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.
--	--

	<ul style="list-style-type: none"> • 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). <p>20. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, powinny zawierać odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).</p> <p>21. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, powinny zawierać odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).</p> <p>22. Rozwiązanie powinno umożliwiać oznaczanie wygenerowanych detekcji jako błędne.</p> <p>23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.</p> <p>24. Rozwiązanie powinno posiadać możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.</p> <p>25. Rozwiązanie powinno pozwalać na dodanie własnego komentarza przy wykrytej detekcji.</p> <p>26. Rozwiązanie powinno umożliwiać wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrótnie administrator powinien otrzymać szczegółowy raport przygotowany przez analityka dotyczący incydentu.</p> <p>27. Rozwiązanie powinno pozwalać na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.</p> <p>28. Rozwiązanie powinno pozwalać na izolację sieciową komputerów przez administratora.</p> <p>29. Rozwiązanie powinno umożliwiać tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.</p> <p>30. Rozwiązanie powinno umożliwiać 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.</p> <p>31. Rozwiązanie powinno umożliwiać tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.</p> <p>32. Rozwiązanie powinno pozwalać na eksport raportów, w postaci plików PDF.</p> <p>33. Rozwiązanie powinno wspierać dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.</p> <p>34. Konsola centralnego zarządzania, powinna posiadać interfejs w języku Polskim.</p>
--	--

35. Konsola zarządzająca powinna być wyposażona jest w panel kontrolny (dashboard) w którym administrator będzie miał możliwość weryfikacji stanu bezpieczeństwa organizacji.
36. Rozwiązanie powinno umożliwiać 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.
37. Konsola powinna być wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR powinna zawierać informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim połączeniu oraz aktualnym statusie.
39. Ochrona antywirusowa powinna być 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 powinno posiadać wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
40. Rozwiązanie powinno wspierać technologię Antimalware Scan Interface (AMSI)
41. Rozwiązanie powinno umożliwiać wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
42. W momencie wykrycia infekcji rozwiązanie powinno automatycznie starać się wyleczyć plik, a jeśli nie jest to możliwe przenieść go do bezpiecznego folderu kwarantanny.
43. Rozwiązanie powinno posiadać możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwalając na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
44. Rozwiązanie powinno chronić plik systemowy HOSTS przed nieautoryzowanymi zmianami.
45. Rozwiązanie powinno posiadać mechanizmy skanujące dyski sieciowe.
46. Skanowanie dysków sieciowych powinno być możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
47. Rozwiązanie powinno posiadać możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
48. Rozwiązanie powinno posiadać mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
49. Powinna istnieć możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
50. Aktualizacje baz definicji wirusów powinny być dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
51. Uaktualnienia definicji wirusów powinny posiadać podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

	<p>52. Rozwiązanie powinno posiadać możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.</p> <p>53. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, powinna następować w sposób automatyczny, niewidoczny dla użytkownika końcowego.</p> <p>54. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie powinna wymagać dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.</p> <p>55. Rozwiązanie powinno posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.</p> <p>56. Rozwiązanie powinno posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.</p> <p>57. Rozwiązanie powinno posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.</p> <p>58. Rozwiązanie powinno posiadać możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.</p> <p>59. Rozwiązanie powinno posiadać możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.</p> <p>60. Rozwiązanie powinno posiadać możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.</p> <p>61. Rozwiązanie powinno posiadać możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.</p> <p>62. Skanowanie dysków przenośnych powinno odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie wyświetlać podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.</p> <p>63. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie powinno wymagać zatrzymania procesu skanowania na jakimkolwiek systemie.</p> <p>64. Rozwiązanie powinno posiadać funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym</p> <p>65. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących powinno odbywać się bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).</p> <p>66. Nie powinien być wymagany restart systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.</p> <p>67. Rozwiązanie powinno posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów.</p>
--	---

	<p>68. Powinno umożliwiać wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.</p> <p>69. Powinno posiadać mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzaną pliki wykonywalne.</p> <p>70. Rozwiązanie powinno posiadać 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 powinny być wysyłane do analizy w infrastrukturze producenta.</p> <p>71. Rozwiązanie powinno posiadać technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanego pliku umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.</p> <p>72. Rozwiązanie powinno posiadać możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanego pliku do dodatkowej analizy przez producenta.</p> <p>73. Rozwiązanie powinno posiadać możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.</p> <p>74. Rozwiązanie powinno posiadać możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.</p> <p>75. Rozwiązanie powinno posiadać 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.</p> <p>76. Rozwiązanie powinno automatycznie powiadamiać użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.</p> <p>77. Rozwiązanie powinno posiadać możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.</p> <p>78. Rozwiązanie powinno posiadać możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.</p> <p>79. Rozwiązanie powinno umożliwiać blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.</p> <p>80. Skanowanie http oraz blokowanie zawartości powinno posiadać możliwość deaktywowania dla witryn określonych, jako zaufane przez system reputacyjny producenta.</p> <p>81. Rozwiązanie powinno posiadać 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.</p> <p>82. Rozwiązanie powinno być wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skryptów ActiveX i pobieranie plików.</p> <p>83. Rozwiązanie powinno posiadać możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.</p>
--	--

84. Rozwiązanie powinno umożliwiać blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
85. Oprogramowanie powinno zapewniać co najmniej 30 kategorii klasyfikacji witryn WWW.
86. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, powinien być powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
87. Rozwiązanie powinno umożliwiać blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
88. Rozwiązanie powinno posiadać wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
89. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie powinno blokować możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
90. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie powinno automatycznie blokować zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
91. Kontrola połączenia powinna umożliwiać zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator powinien mieć możliwość tworzenia własnej listy takich witryn.
92. Rozwiązanie powinno posiadać wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
93. Rozwiązanie powinno posiadać 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.
94. Profile bezpieczeństwa zapory ogniowej powinny zawierać predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
95. Rozwiązanie powinno pozwalać na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
96. Rozwiązanie powinno posiadać możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
97. Rozwiązanie powinno umożliwiać stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
98. Rozwiązanie powinno być wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
99. Mechanizm aktualizacji aplikacji (patch management) nie powinien wymagać instalowania dodatkowych agentów oprócz agenta AV.
100. Moduł aktualizacji aplikacji, powinien okresowo skanować aplikacje zainstalowane na stacji roboczej i umożliwiać ich aktualizację do najnowszych wersji.

101. Moduł aktualizacji aplikacji powinien pełnić rolę mechanizmu łatającego podatności oraz instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
102. Administrator powinien posiadać możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
103. Administrator powinien posiadać możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
104. Mechanizm aktualizacji aplikacji powinien umożliwiać automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
105. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator powinien posiadać możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
106. Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
107. Mechanizm aktualizacji aplikacji (patch management) nie powinien wymagać uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
108. Administrator powinien mieć możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wyłączeń w konsoli zarządzającej.
109. Rozwiązanie powinno umożliwiać wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
110. System centralnego zarządzania powinien prezentować niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
111. Oprogramowanie powinno umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
112. Mechanizm kontroli urządzeń zewnętrznych powinien wspierać między innymi urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
113. Oprogramowanie powinno umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
114. Lista urządzeń zaufanych powinna być tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
115. Rozwiązanie powinno posiadać możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
116. Mechanizm kontroli urządzeń powinien umożliwiać blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
117. Rozwiązanie powinno posiadać opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.

	<p>118. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.</p> <p>119. Rozwiązanie powinno posiadać możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker</p> <p>120. Rozwiązanie powinno pozwalać na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.</p> <p>121. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator powinien posiadać możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.</p> <p>122. Rozwiązanie powinien pozwalać na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.</p> <p>123. Administrator w konsoli zarządzającej powinien posiadać dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.</p> <p>124. Rozwiązanie powinno posiadać wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.</p> <p>125. Mechanizm w swoim działaniu powinien wykorzystywać własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)</p> <p>126. W przypadku wykrycia szkodliwego działania ransomware, moduł powinien blokować aktywność szkodliwego procesu oraz przywracać pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.</p> <p>127. Moduł przywracania plików zaszyfrowanych powinien mieć możliwość działania w trybie monitorowania, bez podejmowania reakcji.</p> <p>128. Administrator powinien mieć możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.</p> <p>129. Administrator powinien posiadać możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.</p> <p>130. Rozwiązanie powinno być wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu powinno polegać na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.</p> <p>131. Moduł powinien posiadać możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.</p> <p>132. Administrator powinien posiadać możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.</p> <p>133. Powinna istnieć możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów powinny mieć możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.</p> <p>134. Rozwiązanie powinno automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz dać możliwość wskazania zaufanych aplikacji przez administratora.</p> <p>135. Rozwiązanie powinno automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz dać możliwość wskazania zaufanych aplikacji przez administratora.</p> <p>136. Rozwiązanie powinno posiadać funkcjonalność kontroli uruchamianych aplikacji.</p>
--	--

	<p>137. Tryb kontroli aplikacji powinien umożliwiać uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.</p> <p>138. Powinna istnieć 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.</p> <p>139. Tworzone reguły powinny dotyczyć czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.</p> <p>140. Na wspieranych systemach Windows rozwiązanie powinno pozwalać na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.</p> <p>141. Administrator powinien posiadać w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN</p> <p>142. Rozwiązanie powinno pozwalać 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)</p> <p>143. Administrator powinien mieć możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.</p> <p>144. Rozwiązanie powinno pozwalać na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).</p> <p>145. Wygenerowany plik powinien mieć możliwość otwarcia i wykorzystania do zdalnego połączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.</p> <p>Centralna administracja</p> <ol style="list-style-type: none"> 1. Portal zarządzający powinien być dostępny w języku polskim. 2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi powinna się odbywać w formie zaszyfrowanej. 3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie powinna być 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. 4. Interfejs zarządzania powinien posiadać funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadomienia o zakończeniu licencji. 5. Interfejs powinien być wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 6. Wykresy powinny być interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
--	--

	<ol style="list-style-type: none"> 7. Rozwiązanie powinno posiadać dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Powinna istnieć możliwość eksportu listy wszystkich hostów do pliku CSV. 9. Administrator powinien posiadać 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. 10. Administrator powinien mieć 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. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie powinno posiadać dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Powinna istnieć możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego powinny zawierać liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator powinien posiadać możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana. 16. Administrator powinien posiadać możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie powinno posiadać moduł raportujący, w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty powinny być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie powinno posiadać wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator powinien widzieć w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. Portal zarządzający powinien umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365. 22. Dodanie klucza licencyjnego powinno skutkować pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie powinno mieć możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
--	---

	<p>24. Profile powinny posiadać możliwość przypisania do pojedynczych hostów lub do grup.</p> <p>25. Profile powinny posiadać możliwość automatycznego przypisywania do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.</p> <p>26. W przypadku automatycznego przypisywania profili, system powinien pozwalać na automatyczne dodawanie tagów dla hostów, które otrzymają dany profil konfiguracyjny.</p> <p>27. Powinna istnieć możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.</p> <p>28. Rozwiązanie powinno pozwalać 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.</p> <p>29. Z poziomu portalu zarządzającego powinna istnieć możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.</p> <p>30. Pliki instalacyjne mają posiadać rozszerzenia plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.</p> <p>31. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.</p> <p>32. Administrator powinien posiadać możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.</p> <p>33. Powinno być dostępne dla Administratora 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.</p> <p>34. Portal zarządzający powinien pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.</p> <p>35. Konsola powinna posiadać możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.</p> <p>36. W ramach posiadanych licencji powinna istnieć możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji</p>
<p>Certyfikaty i standardy – dokumenty należy załączyć wraz z ofertą lub na wezwanie Zamawiającego</p>	<p>1. Oferowane rozwiązanie klasy Endpoint Protection Platform (EPP) powinno być rozwiązaniem uznanym na rynku, co oznacza, że zostało uwzględnione w aktualnych raportach analitycznych dotyczących rynku bezpieczeństwa IT, takich jak Gartner Magic Quadrant, Forrester Wave lub równoważnych opracowaniach potwierdzających pozycję rynkową i dojrzałość oferowanego rozwiązania. Zamawiający dopuszcza spełnienie wymagań certyfikacyjnych łącznie lub równoważnie, poprzez przedstawienie zestawu certyfikatów i raportów potwierdzających porównywalny poziom bezpieczeństwa i dojrzałości rozwiązania.</p>

	<p>2. Oferowane rozwiązanie musi należeć do klasy Endpoint Protection Platform (EPP) i spełniać wymagania funkcjonalne określone dla tej klasy rozwiązań, w szczególności w zakresie:</p> <ul style="list-style-type: none"> a) ochrony przed złośliwym oprogramowaniem (malware), b) wykrywania zagrożeń typu zero-day, c) ochrony przed ransomware, d) centralnego zarządzania i raportowania, e) mechanizmów EDR/XDR , <p>3. Zamawiający dopuszcza rozwiązania równoważne, pod warunkiem wykazania przez Wykonawcę, że oferowany produkt spełnia wymagania funkcjonalne i jakościowe nie gorsze niż rozwiązania wskazane w powyższych raportach.</p>
Rozszerzone wsparcie serwisowe	<ul style="list-style-type: none"> 1. System powinien być objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. 2. System powinien być objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: <ul style="list-style-type: none"> a) Wsparcie telefoniczne zespołu certyfikowanych inżynierów. b) Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. c) Doradztwo w zakresie konfiguracji. d) Zdalne wsparcie techniczne. e) Pomoc w zakładaniu zgłoszeń serwisowych u producenta. f) Przygotowanie do zdalnej konfiguracji. g) Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. h) Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. i) Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. j) Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. 3. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe powinien być przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. 4. Oferent winien przedłożyć dokumenty: <ul style="list-style-type: none"> a) Oświadczenie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). b) Certyfikat ISO 9001:2015 oraz 27001 autoryzowanego podmiotu serwisującego. (dołączyć do oferty).

	c) Certyfikat inżynierski potwierdzony przez Producenta dla min. dwóch osób w zakresie produktów: EDR/XDR oraz skaner podatności (dołączyć do oferty).
Wymagania specjalne dla wersji mobilnej oprogramowania (5 szt.)	<ol style="list-style-type: none"> 1. Oprogramowanie powinno zapewniać ochronę oraz możliwość egzekwowania polityk bezpieczeństwa dla urządzeń mobilnych z systemami Android oraz iOS. 2. Rozwiązanie powinno zapewniać co najmniej następujące dodatkowe funkcjonalności: <ol style="list-style-type: none"> 1) Kontrola i ochrona ruchu sieciowego (bramka sieciowa) <ol style="list-style-type: none"> a) Oprogramowanie powinno umożliwiać kontrolę ruchu sieciowego urządzenia oraz weryfikację reputacji odwiedzanych adresów URL przed załadowaniem strony. b) Oprogramowanie powinno umożliwiać blokowanie stron złośliwych. c) Oprogramowanie powinno umożliwiać opcjonalne blokowanie stron należących do wybranych kategorii treści (np. treści dla dorosłych, hazard). d) Oprogramowanie powinno umożliwiać rejestrowanie/raportowanie zdarzeń bezpieczeństwa (np. próby wejścia na strony zablokowane) w konsoli administracyjnej. e) Oprogramowanie powinno umożliwiać konfigurację widoczności danych o odwiedzanych adresach URL w konsoli administracyjnej w celu dostosowania do przepisów dot. prywatności (z zastrzeżeniem, że Zamawiający odpowiada za zgodność przetwarzania danych z przepisami prawa). f) Oprogramowanie powinno zapewniać spójny poziom ochrony dla iOS i Android. Dla iOS powinno zapewniać integrację z przeglądarką Safari oraz współpracę z istniejącymi konfiguracjami VPN, jeżeli są stosowane. 2) Analiza zagrożeń w chmurze (Security Cloud) <ol style="list-style-type: none"> a) Oprogramowanie powinno wykorzystywać chmurową analizę zagrożeń w czasie rzeczywistym w celu identyfikacji, analizy oraz zapobiegania nowym lub pojawiającym się zagrożeniom. b) Oprogramowanie powinno umożliwiać skanowanie pobieranych plików/aplikacji (w tym pakietów instalacyjnych Android, np. APK) oraz sprawdzanie ich reputacji w usłudze chmurowej. c) Oprogramowanie powinno blokować uruchomienie plików/aplikacji uznanych za złośliwe. d) Oprogramowanie powinno umożliwiać przesyłanie nieznanych plików/aplikacji do pogłębionej analizy (jeżeli funkcja jest dostępna i dopuszczalna organizacyjnie).

	<p>3) Ochrona aplikacji i treści (Android)</p> <ul style="list-style-type: none"> a) Oprogramowanie powinno chronić urządzenia przed złośliwym oprogramowaniem i złośliwą zawartością z wykorzystaniem mechanizmów skanowania ruchu na poziomie sieci. b) Dla systemu Android oprogramowanie powinno dodatkowo umożliwiać lokalne skanowanie oraz weryfikację reputacji w czasie rzeczywistym. <p>4) Ochrona przeglądania (anty-phishing / anty-malware w WWW)</p> <ul style="list-style-type: none"> a) Oprogramowanie powinno uniemożliwiać użytkownikom odwiedzanie złośliwych witryn (w tym phishingowych) oraz ograniczać ryzyko wejścia na złośliwe strony przez linki w wiadomościach e-mail, reklamy lub przekierowania. b) Ochrona przeglądania powinna działać niezależnie od używanej przeglądarki (np. na poziomie sieci). c) Oprogramowanie powinno wykorzystywać aktualne dane reputacyjne (np. adresy IP, cechy URL, zachowanie witryn) w celu podejmowania decyzji o blokowaniu/zezwalaniu. <p>5) Ograniczanie śledzenia i optymalizacja transmisji (opcjonalnie)</p> <p>Oprogramowanie powinno oferować funkcje ograniczania śledzenia online (anti-tracking) oraz może oferować mechanizmy optymalizacji transmisji danych (np. kompresję ruchu), przy zachowaniu minimalnego wpływu na wydajność urządzenia i zużycie baterii.</p> <p>6) Wdrożenie i współpraca z systemami MDM</p> <p>6.1 Oprogramowanie powinno umożliwiać wdrożenie i konfigurację za pośrednictwem rozwiązań MDM/EMM firm trzecich.</p> <p>6.2 Oprogramowanie powinno wspierać co najmniej następujące systemy MDM:</p> <ul style="list-style-type: none"> a) VMware Workspace ONE b) IBM Security MaaS360 c) Google Workspace MDM d) Microsoft Intune e) Miradore f) Ivanti Endpoint Manager g) Samsung Knox <p>7) Zarządzanie centralne (konsola w chmurze)</p> <p>7.1 Oprogramowanie powinno zapewniać centralne zarządzanie politykami bezpieczeństwa oraz widoczność statusu ochrony urządzeń w konsoli administracyjnej (hostowanej w chmurze).</p> <p>7.2 Oprogramowanie powinno umożliwiać obsługę procesu zapraszania użytkowników/urządzeń do instalacji:</p> <ul style="list-style-type: none"> a) zaproszenia widoczne w konsoli do czasu zakończenia instalacji, b) link instalacyjny unikalny i jednorazowy, c) możliwość ponownego wysłania zaproszenia oraz wygenerowania nowego linku po wygaśnięciu, d) ważność linku instalacyjnego ograniczona czasowo (np. do 30 dni).
--	--

2.2. Wdrożenie oprogramowania typu EDR/XDR do integracji z SIEM

Wykonawca zrealizuje wdrożenie oprogramowania typu EDR/XDR do integracji z SIEM w uzgodnionym z Zamawiającym terminie, w formule umożliwiającej realizację prac stacjonarnie oraz zdalnie, o ile warunki techniczne i bezpieczeństwa po stronie Zamawiającego na to pozwolą (w szczególności zapewnienie zdalnego dostępu dla Wykonawcy zgodnie z obowiązującymi u Zamawiającego zasadami). Przed rozpoczęciem prac wdrożeniowych Zamawiający przygotuje niezbędne elementy do wdrożenia, w tym w szczególności: infrastrukturę/środowisko (serwer/VM lub zasoby chmurowe – zgodnie z przyjętym modelem wdrożenia), dostęp sieciowy pomiędzy komponentami, konta i uprawnienia administracyjne wymagane do instalacji i konfiguracji, a także listę programów współpracujących z EDR/XDR przewidzianych do podłączenia wraz z informacją o sposobie ich połączenia oraz osoby kontaktowe po stronie Zamawiającego odpowiedzialne za udostępnienie dostępu i wsparcie integracji. Wykonawca musi spełnić wszystkie ww. wymagania Zamawiającemu, niezbędne do prawidłowego przeprowadzenia wdrożenia min. 14 dni przed planowanym wdrożeniem.

1. W ramach wdrożenia Wykonawca przeprowadzi instalację i konfigurację oprogramowania typu EDR/XDR do integracji z SIEM podłączy uzgodnione źródła danych oraz skonfiguruje podstawowe elementy działania systemu w zakresie wymaganym OPZ. Po zakończeniu konfiguracji Wykonawca przygotuje i przeprowadzi wspólnie z Zamawiającym testy działania obejmujące weryfikację poprawności zbierania danych ze wskazanych źródeł, podstawowej poprawności przetwarzania oraz działania skonfigurowanych mechanizmów alertowania i prezentacji; scenariusze testowe zostaną uzgodnione z Zamawiającym i będą stanowiły podstawę odbioru wdrożenia. Wdrażanie należy przeprowadzić w sposób, który nie zakłóci ciągłości działania. Harmonogram wdrażania powinien obejmować jednorazowo nie więcej niż 10% systemów IT oraz ustawienie agend XDR w trybie monitorującym do czasu przetestowania stabilności aplikacji, sprawdzenia wydajności i pracy urządzeń i sieci IT. Po zakończeniu konfiguracji Wykonawca przygotuje i przeprowadzi wspólnie z Zamawiającym testy działania obejmujące weryfikację poprawności zbierania danych ze wskazanych źródeł, podstawowej poprawności przetwarzania oraz działania skonfigurowanych mechanizmów alertowania i prezentacji. Wykona testy detekcji przykładowych scenariuszy ataków (np. malware, ransomware, lateral movement) oraz wykona testy mechanizmów reakcji (alertowanie, izolacja, blokowanie). Scenariusze testowe zostaną uzgodnione z Zamawiającym i będą stanowiły podstawę odbioru wdrożenia. Wykonawca przeprowadzi szkolenie dla wskazanych przez Zamawiającego dla administratorów (3 osób) w zakresie konfiguracji i bieżącej obsługi oferowanego rozwiązania w zadaniu 1 i 2, w języku polskim, wraz z przekazaniem materiałów szkoleniowych. Szkolenie musi być zakończone potwierdzającym umiejętności certyfikatem.

Po odbiorze wdrożenia Wykonawca zapewni dodatkowe wsparcie powdrożeniowe przez okres gwarancji realizowane zdalnie, obejmujące konsultacje oraz wprowadzanie

uzgodnionych korekt konfiguracyjnych wynikających z eksploatacji rozwiązania w środowisku Zamawiającego (w szczególności w zakresie działania integracji oraz konfiguracji elementów, które były przedmiotem wdrożenia). Wszystkie wymienione powyżej prace muszą zostać wykonane w obecności przedstawiciela Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po wykonanych pracach wdrożeniowo – instalacyjnych w godzinach od 7.00 do 15.00.

W tym czasie przedstawiciel Wykonawcy:

- a. zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji.
- b. dokona prezentacji działania systemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności zastosowanych rozwiązań aplikacyjnych.

Wykonawca zobowiązany jest do:

- a. zapewnienia punktu kontaktowego (Service Desk),
- b. usuwania awarii, błędów oraz nieprawidłowości działania systemu,
- c. pomoc w konfiguracji i dostrajaniu polityk detekcji oraz reakcji,
- d. wsparcie Zamawiającego w interpretacji alertów i incydentów bezpieczeństwa generowanych przez system XDR,
- e. korektę konfiguracji w przypadku zmian w środowisku IT Zamawiającego,
- f. aktualizacji systemu XDR, agentów oraz sygnatur detekcji,
- g. współpracy z zespołem IT Zamawiającego w zakresie integracji XDR z innymi systemami bezpieczeństwa (NGFW, VPN, MFA, SIEM,
- h. współpracy z Zamawiającym w przypadku incydentów o podwyższonym poziomie krytyczności,
- i. prowadzenia doradztwa technicznego w zakresie optymalnego wykorzystania funkcjonalności systemu XDR.

Gwarancja, o której mowa w SOPZ, stanowi element umowy sprzedaży lub wykonania prac i nie jest usługą wsparcia ani utrzymania systemu. Realizacja gwarancji nie stanowi odrębnego świadczenia odpłatnego.

