Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

„System Nadzoru Cyberbezpieczeństwa”

1. Cel i przedmiot Zamówienia

Przedmiotem zamówienia jest dostawa zestawu niezbędnych licencji oraz wykonanie wdrożenia i konfiguracji Systemu Nadzoru Cyberbezpieczeństwa (dalej System NC) w środowisku produkcyjnym Zamawiającego, zgodnie z Harmonogramem Wdrożenia, a także realizacja uprawnień Zamawiającego wynikająca z Gwarancji Producenta licencji oraz Gwarancji Wykonawcy, a także świadczenie usług Asysty Powdrożeniowej przez Wykonawcę.

Głównym celem Systemu NC jest znaczące podniesienie poziomu bezpieczeństwa cyfrowego w infrastrukturze IT Zamawiającego poprzez dostawę, pełne i skuteczne wdrożenie licencji w oparciu o najlepsze praktyki branżowe, pozwalające na co najmniej: efektywne wykrywanie i reagowanie na podejrzany ruchu sieciowy, ochronę przed atakami m.in. "zero-day", „ransomware”, zapewnienie nadzoru wykonania programów i integralności konfiguracji, (XDR/EDR), wprowadzeniem mechanizmów przeciwdziałania wyciekom danych (DLP) i zarządzania szyfrowaniem stacji roboczych, wdrożenie rozwiązań zarządzania dostępem uprzywilejowanym (PAM) oraz umożliwienie monitorowania w trybie ciągłym zasobów IT, z wykorzystaniem nowoczesnych mechanizmów analizy i korelacji zdarzeń, a także umożliwienie zarządzania i automatyzacji realizacji działań zaradczych.

2. Ramowy plan dostawy i wdrożenia licencji Systemu NC oraz realizacji usługi Asysty Powdrożeniowej.

ETAP I - Rozpoczęcie projektu, analiza zakresu i przygotowanie planu wdrożenia.

1. Wykonanie analizy przedwdrożeniowej zakończonej projektem Systemu NC.
2. Przygotowanie założeń umożliwiających Odbiór Końcowy Systemu NC.
3. Opracowanie planu wdrożenia i odbioru, uwzględniającego konieczność zachowania ciągłości działalności Zamawiającego.

ETAP II – Wdrożenie i konfiguracja Systemu Nadzoru Cyberbezpieczeństwa w ramach infrastruktury IT Zamawiającego i osiągnięcie gotowości do Odbioru Końcowego.

1. Instalacja i w wstępna konfiguracja przedmiotowych licencji oprogramowania.
2. Wykonanie dalszych niezbędnych konfiguracji w celu osiągnięcia zakładanej spójności i efektywności posiadanych przez Zamawiającego rozwiązań sprzętowo-systemowych z Systemem NC.
3. Wykonanie prac i konfiguracji niezbędnych do osiągnięcia przez Wykonawcę gotowości do Odbioru Końcowego Systemu NC.
4. Wykonanie zestawu testów demonstracyjnych w ramach oprogramowania typu SIEM, umożliwiających Zamawiającemu przygotowanie się do Odbioru Końcowego.
5. Dostrojenie Systemu NC na bazie wykonanych testów demonstracyjnych i zgłoszonych uwag Zamawiającego.

6. Dostarczenie niezbędnych licencji wymaganych do uzyskania pełnej funkcjonalności Systemu NC.

ETAP III - Odbiór Końcowy potwierdzający uzyskanie wymaganej konfiguracji, integracji i funkcjonalności Systemu Nadzoru Cyberbezpieczeństwa.

1. Wykonanie serii końcowych scenariuszy testowych potwierdzających prawidłowe wykonanie Systemu NC.
2. Przekazanie majątkowych praw autorskich do Oprogramowania Dedykowanego i pełnej konfiguracji Sytemu NC powstałego w trakcie wdrożenia.
3. Dostarczenie dokumentacji powdrożeniowej.

ETAP IV - Asysta Powdrożeniowa na warunkach wskazanych w OPZ i Umowie przez 12 miesięcy.

1. Świadczenie usług Asysty Powdrożeniowej przez Wykonawcę od momentu podpisania Protokołu Odbioru Końcowego przez okres 12 miesięcy.
2. Wykonanie aktualizacji w dokumentacji powdrożeniowej z Etapu III.
3. Przekazanie majątkowych praw autorskich do Rezultatów Prac, w tym do Oprogramowania Dedykowanego powstałego wskutek realizacji działań w czasie realizacji usługi Asysty Powdrożeniowej, na zakończenie realizacji usługi.

Wdrożenie zostanie przeprowadzone w Etapach I-II z zgodnie z Ramowym Harmonogramem Wdrożenia (Załącznik nr 8).

Wymagania dotyczące funkcjonalności zestawu licencji Systemu Nadzoru Cyberbezpieczeństwa

System Nadzoru Cyberbezpieczeństwa składa się z niżej wymienionych i opisanych komponentów składowych, Oprogramowania Dedykowanego powstałego w trakcie wdrożenia, w tym wszelkich nowych lub zaktualizowanych konfiguracji, tak aby umożliwić Zamawiającemu Odbiór Końcowy i korzystanie z Systemu NC oraz świadczenie usług Asysty Powdrożeniowej.

3. Wymagania dla podsystemu ochrony hostów, serwerów i urządzeń mobilnych (System OHSM)

1) Dostarczenie zestawu niezbędnych licencji wraz z ich wdrożeniem, uprawniających Zamawiającego do jednoczesnej ochrony **300 hostów/stacji roboczych** (typu laptop, komputer), **50 serwerów (fizycznych lub zwirtualizowanych)** oraz **50 urządzeń mobilnych**, a także analizy i reagowania na podejrzany ruch sieciowy. Licencje co niemniej trzyletnie, muszą uprawniać Zamawiającego do uzyskiwania dostępu i aktualizacji do wykorzystywanych lub przetwarzanych danych zewnętrznych do realizacji celów Systemu OHMS przez okres min. 36 miesięcy od zakończenia wdrożenia licencji, potwierdzonego Protokołem Odbioru Końcowego.
2) System OHSM musi składać się ze spójnie funkcjonujących komponentów:

   a. Agentów ochrony instalowanych w systemach operacyjnych na stacjach roboczych oraz serwerach.
   b. Agentów ochrony dedykowanych dla urządzeń mobilnych (funkcjonalność MDM)
   c. Oprogramowanie sond sieciowych monitorujących podejrzany ruch sieciowy (funkcjonalność XDR-Network).
   d. Pozostałych niezbędnych komponentów takich jak: agenci dla kontrolerów domeny Microsoft Active Directory, bramy proxy dla usług działających w infrastrukturze IT Zamawiającego oraz aplikacji mobilnej wspierającej pracę administratorów Systemu OHMS.
   e. Konsoli zarządzającej dla hostów/stacji roboczych dostępnej on-premise z możliwością migracji do chmury producenta w Europejskim Obszarze Gospodarczym.
3) System OHMS musi mieć możliwość przechowywania danych telemetrycznych przez minimum 30 dni.
4) System OHMS musi zapewniać wsparcie dla systemów operacyjnych:
   a. Microsoft Windows: (Windows Server 2012R2, 2016, 2019 i 2022 w wersjach 64-bit).
   b. Linux: (Debian 9 i nowsze (64-bit), Ubuntu 16 i nowsze (64-bit oraz ARM), CentOS Linux 6 i nowsze (64-bit)).
   c. MacOS Big Sur (11.0) i nowsze (procesory Intel oraz Apple).
5) System OHMS musi posiadać certyfikacje potwierdzające zgodność z najlepszymi praktykami w zakresie przetwarzania i bezpieczeństwa danych tj.: CSA Star Level 2, FedRAMP, ISO 27001, 27014, 27034 oraz ISO 27017, PCI DSS Certified Service Provider, SOC 3, SOC 2 Type II.
6) System OHMS musi umożliwiać integracje z systemami firm trzecich za pomocą interfejsu programowania aplikacji API.
7) System OHMS musi umożliwiać eksportowanie alertów oraz logów audytowych w standardowym formacie syslog.
8) Systemu musi posiadać wbudowane (tj. wykonane przez producenta) mechanizmy integracji z następującymi produktami i usługami:
   a. SIEM – w celu przekazywanie alertów - min. Elastic i Microsoft Sentinel.
   b. Systemy firewall i bramy webowe – w celu blokowania zdarzeń wykrytych przez moduł XDR – co najmniej dla rozwiązań FortiGate, które posiada Zamawiający.
   c. Systemy ITSM – w celu automatycznego kreowania zgłoszeń dla administratorów na podstawie alertów z modułu XDR – min. Jira.
   d. Systemy threat intelligence – w celu wymiany danych typu IoC (Indicators of Compromise) tj. dowodów na to, że ktoś mógł naruszyć bezpieczeństwo sieci lub chronionych urządzeń.
   e. Integracja z usługą Virus Total – w celu automatycznego wzbogacania informacji o zagrożeniach na podstawie danych przesłanych i otrzymanych z Virus Total API.
9) System musi posiadać wbudowany własny moduł obsługi zgłoszeń (case management).
10) System musi umożliwiać przypisanie otwartego zgłoszenia do wybranego analityka.
11) System musi umożliwiać nadawanie zgłoszeniom priorytetów, w przypadku otwarcia zgłoszenia o najwyższym priorytecie musi istnieć możliwość automatycznego powiadamiania przydzielonych analityków przez email oraz aplikację mobilną
12) Do otwartych zgłoszeń musi istnieć możliwość dodania notatek i załączników (w formie plików).

13) Musi istnieć możliwość otwarcia zgłoszenia w systemie z poziomu wygenerowanego alertu i przypisania do niego właściciela.
14) Dedykowana aplikacja mobilna administratorów musi posiadać ograniczone uprawnienia, bez możliwości wprowadzania zmian w systemie.
15) Musi istnieć możliwość podejrzenia ostatnich alertów oraz ich statusu oraz listy otwartych zgłoszeń wraz z ich historią.
16) Aplikacja mobilna musi generować powiadomienia na urządzeniu mobilnym w przypadku wykrycia przez system zagrożenia, z podaniem poziomu krytyczności (niski, średni, wysoki, krytyczny) oraz krótkiego opisu zdarzenia.
17) Musi istnieć możliwość konsolidowania powiadomień dla aplikacji mobilnej, dotyczących alertów o niskim poziomie krytyczności w okresie jednej godziny.
18) Logowanie do konsoli zarządzającej oraz aplikacji mobilnej musi wymagać użycia drugiego składnika - MFA (multi-factor authentication).
19) Musi istnieć możliwość ograniczenia logowania do konsoli zarządzającej do wybranych źródłowych zakresów adresów IP.
20) Konsola zarządzająca musi umożliwiać nadawanie uprawnień dla administratorów na podstawie ról (RBAC, Role Based Access Control).
21) Na system oraz wszystkie jego moduły muszą być objęte min. 3 letnią licencją uprawniającą do uzyskiwania aktualizacji i wsparcia producenta przez okres min. 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego.

3.1. Funkcjonalność ochrony XDR

1) Moduł jest odpowiedzialny za generowanie alertów na podstawie danych telemetrycznych zebranych ze stacji roboczych oraz serwerów.
2) Moduł musi przetwarzać dane telemetryczne w zakresie co najmniej:
    a. Procesów i ich zmian w systemie operacyjnym.
    b. Plików, w tym zapisu, kopiowania, modyfikacji, pobierania z Internetu w raz z ich sumami kontrolnymi (MD5, SHA1, SHA256).
    c. Ruchu sieciowego, w tym zapytań DNS, przychodzących i wychodzących połączeń sieciowych, otwieranych portów, adresów IP.
    d. Operacji na rejestrze (w systemach MS Windows).
    e. Zdarzeń z logów systemowych.
    f. Zdarzeń wynikających z dodatkowych funkcjonalności modułu ochrony stacji roboczych.
3) Moduł musi mieć możliwość przeszukiwania zgromadzonych surowych danych telemetrycznych.
4) Wyszukiwanie musi zwracać surowe dane w formie tabelarycznej, z wizualizacją odnalezionych zdarzeń na osi czasu.
5) Wyszukiwarka musi umożliwiać dynamiczne tworzenie widoków, z możliwością wyboru odpowiednich kolumn w tabeli wyników.
6) Wyszukiwarka musi umożliwiać zapisywanie stworzonych dynamicznych widoków oraz ich ponowne zastosowanie po wyborze z listy rozwijanej.
7) Musi istnieć możliwość zapisania stworzonego zapytania do wyszukiwarki oraz podgląd historii zapytań.

8) Wyszukiwarka musi umożliwiać zdefiniowanie przedziału czasowego, dla którego zwracane będą wyniki.
9) Musi istnieć możliwość eksportowania wyników wyszukiwania w formacie JSON.
10) Moduł musi automatycznie generować zdarzenia na podstawie zebranych danych telemetrycznych, w przypadku wykrycia zagrożenia Zdarzenia muszą posiadać odpowiedni opis, z uwzględnieniem poziomu ich krytyczności (w pięciostopniowej skali) oraz z mapowaniem na taktyki i techniki zgodnie z macierzą Mitre ATT&CK.
11) Moduł musi umożliwiać, dla każdego z wygenerowanych zdarzeń, uruchomienie zapytania do asystenta AI, opartego o wytrenowany przez producenta Modułu model LLM, w celu wygenerowania prostego opisu (wyjaśnij zdarzenie) wraz z krótkim podsumowaniem, rekomendowanymi akcjami naprawczymi oraz zalecanymi następnymi krokami do podjęcia w celu głębszej analizy zdarzenia.
12) W przypadku wygenerowania kilku różnych zdarzeń dla pojedynczego urządzenia i podobnego okresu czasu, Moduł powinien automatycznie je korelować i sortować według przypisanego poziomu krytyczności.
13) Moduł musi posiadać stworzony przez producenta zestaw modeli detekcyjnych, korelujących zdarzenia.
14) Modele detekcyjne muszą generować alerty i prezentować je w przystępny sposób, z użyciem grafów, umożliwiając lepsze zrozumienie sytuacji.
15) Grafy powinny zawierać najważniejsze elementy zidentyfikowane jako podejrzane, istotne do analizy wykrytego ataku, w tym:
    a. Maszyny.
    b. Konta użytkowników.
    c. Adresy IP.
    d. Wywołania linii komend.
    e. Powołane procesy.
    f. Pliki.
    g. Klucze rejestru (dla systemów MS Windows).
16) Moduł musi umożliwiać, na żądanie administratora, przygotowanie grafu obrazującego powiązania zdarzeń w systemie operacyjnym (dotyczących procesów, plików, połączeń sieciowych), związanych z analizowanym alertem.
17) Graf powinien obrazować wzajemne relacje obiektów (np. dany proces stworzył plik wykonywalny, z pliku wykonywalnego został powołany nowy proces potomny, który nawiązał komunikację sieciową do konkretnych adresów IP, etc.)
18) Z poziomu alertu musi istnieć możliwość podjęcia działań naprawczych, w tym:
    a. Izolacji wybranej stacji, której dotyczy alert.
    b. Zakończenia podejrzanego procesu
    c. Dodania obiektu (adresu IP, pliku, adresu URL do listy zablokowanych obiektów)
    d. Pobrania pliku do konsoli
    e. Przekazania pliku do analizy w bezpiecznym środowisku (sandbox).
    f. Uruchomienia zdalnej sesji do analizowanej maszyny.
    g. Wykonania skryptu (powershell dla systemu Windows, bash dla systemów Linux).
    h. Wyszukania wybranego obiektu w zgromadzonych danych telemetrycznych
19) Z poziomu alertu musi istnieć możliwość automatycznego wygenerowania zapytania do wyszukiwarki danych telemetrycznych, w celu przeprowadzenia dalszej analizy. Zapytanie powinno zwracać wszystkie zdarzenia z wybranej stacji w zadanym czasie przed i po czasie powstania analizowanego alertu (np. +/- 5 min).

20) Alerty, które spełniają kryteria podobieństwa (dla czasu wystąpienia, źródła, przebiegu) muszą zostać automatycznie połączone i opisane w formie incydentu.
21) Musi istnieć możliwość ręcznego przypisywania wybranych alertów do widoku incydentu.
22) Funkcjonalność modułu Threat Intelligence:
    a. Moduł Threat Intelligence musi umożliwiać automatyczne pobieranie informacji o zagrożeniach - IoC (*Indicators of Compromise*) w następujący sposób:
        i. Poprzez wbudowaną integrację z platformą MISP (https://www.misp-project.org)
        ii. Poprzez protokół TAXII (Trusted Automated eXchange of Intelligence Information) w wersji 2.0 oraz 2.1.
        iii. Ręcznie poprzez import pliku w formacie STIX (Structured Threat Information Expression)
        iv. Ręcznie poprzez import pliku w formacie .csv.
    b. Istnieje możliwość importu poniższych typów IoC:
        i. Nazwa domenowa;
        ii. Hash (SHA-1, SHA-256);
        iii. Adres IP;
        iv. URL;
        v. Adres email nadawcy.
    c. Umożliwia przeprowadzanie automatycznego skanowanie danych telemetrycznych w poszukiwaniu wprowadzonych IoC. Skanowanie musi odbywać się od razu po wprowadzeniu danych oraz cyklicznie co najmniej przez siedem kolejnych dni od daty importu, a także umożliwi ręczne uruchomienie skanowania w poszukiwaniu wprowadzonych IoC.
    d. Funkcjonalność automatycznego blokowania oraz logowania pobranych IoC przez komponenty modułu ochrony anty-malware, a także automatycznego usuwania starych IoC - po upływie określonego przez administratora czasu.
23) Moduł musi umożliwiać szczegółowe raportowanie wszystkich akcji oraz zapewniać możliwość generowania wykresów/diagramów/zestawień (logiczne filtrowanie informacji).
24) Wymagane jest, aby funkcjonalność antymalware do ochrony przed zaawansowanymi zagrożeniami realizowana była przez co najmniej następujące mechanizmy detekcji:
    a. Sygnaturowej.
    b. Heurystycznej.
    c. Behawioralnej.
    d. Uczenia maszynowego (machine learning).
25) Funkcjonalność ochrony musi realizować:
    a. skanowanie stacji w trybach: zgodnie z harmonogramem, na żądanie oraz w czasie rzeczywistym;
    b. filtrowanie ruchu WWW (http/https) na podstawie reputacji adresów URL - baza reputacyjna musi być dostarczana i aktualizowana przez producenta w okresie wsparcia zaś filtrowanie musi odbywać się bez konieczności instalacji dodatkowych wtyczek do przeglądarek internetowych (Chrome, Firefox, Edge, Safari);
    c. przeciwdziałanie atakom wykorzystującym skrypty oraz misi integrować się z mechanizmem AMSI (Anti Malware Scan Interface) w systemach MS Windows.
    d. funkcjonalność auto-ochrony agenta poprzez zdefiniowanie hasła wymaganego do jego odinstalowania w systemach MS Windows.
    e. ochronę przed atakami i zagrożeniami typu ransomware;

f. funkcjonalność wykonywania w pamięci kopii zapasowej plików, z których korzysta użytkownik; wielkość kopii zapasowej, oraz typy plików nią obejmowane muszą być definiowalne przez administratora po stronie konsoli centralnego zarządzania (dopuszcza się funkcję anty-ransomare realizowaną w autorski sposób producenta, bez wykorzystania kopii zapasowej plików). Utworzenie kopii konkretnych plików może być realizowane w momencie wykrycia działania;
g. automatyczne usuwanie lub blokowanie wirusów oraz alarmowanie w przypadku wykrycia zagrożenia poprzez centralną kontrolę zarządzania;
h. wykrywanie skanowania portów.

26) Moduł ochrony stacji końcowych musi umożliwiać realizowanie kontroli aplikacji (application control) dla stacji z zainstalowanym systemem Windows poprzez co najmniej następujące funkcje:
    a. zdefiniowanie zestawu aplikacji, które użytkownik końcowy będzie mógł uruchomić, zaś pozostałe aplikacje powinny być blokowane;
    b. ochronę przed uruchamianiem niepożądanych lub nieznanych aplikacji, plików wykonywalnych, bibliotek DLL, aplikacji MS Windows, sterowników urządzeń, oraz innych przenośnych plików wykonywalnych (Portable Executable Files);
    c. analiza zagrożeń w czasie rzeczywistym bazujący na globalnej bazie reputacji plików;
    d. definiowanie i wykorzystywanie polityk zawierających zdefiniowane reguły dot. metod kontroli aplikacji:
        - „Zezwól” (Allow) – reguły zezwalające na uruchomienie określonych, wyspecyfikowanych aplikacji,
        - „Blokuj” (Block) – reguły blokują określone, wybrane aplikacje lub aplikacje nie określone w regułach typu „Allow”,
        - „Izolacja” (Lockdown) – blokuje aplikacje dodane po zastosowaniu reguły typu „Lockdown” z możliwością użycia określonych warunków na zezwolenie uruchomienia tych aplikacji.
27) Moduł ochrony musi mieć wbudowany mechanizm ochrony przed atakami na znane podatności, pochodzącymi z sieci (typu host IPS).
28) Moduł ochrony musi posiadać zestaw dostarczanych i na bieżąco aktualizowanych przez producenta systemu, gotowych do użycia sygnatur.
29) Funkcjonalność ochrony w zakresie zabezpieczenia przed wyciekiem wrażliwych danych (DLP) - monitorowanie i powiadamianie o incydentach wycieku danych w czasie rzeczywistym:
    a. przy wykorzystaniu co najmniej takich mechanizmów jak:
        i. wyrażenia regularne, atrybuty plików, słowa kluczowe (konfigurowalna lista słów wrażliwych i wyrażeń);
        ii. gotowe, dostarczane przez producenta szablony wyrażeń regularnych pozwalające na kontrolę i ochronę danych typowych dla Polski (np.: numer dowodu osobistego, numer PESEL, numer rachunku bankowego);
    b. poprzez monitorowanie i ochronę kanałów transmisji:
        i. poczta elektroniczna (oprogramowanie klienckie – min. MS Outlook, Thunderbird);
        ii. poczta elektroniczna dostępna poprzez przeglądarkę WWW (webmail);
        iii. protokoły HTTP i HTTPS;
        iv. protokół SMB;
        v. nagrywarki (CD/DVD);
        vi. aplikacje wymiany plików peer-to-peer;

vii. drukarki;
viii. schowek systemu Windows.

c. w przypadku wykrycia naruszenia polityki ochrony przed wyciekiem poufnych danych dostępne są funkcjonalności pozwalające na podjęcie akcji (wymienione niżej) oraz niezależnie od wybranej akcji – zostaną zapisane dane i oznaczone jako naruszenie polityki w celu dalszej analizy:
   i. „Pomiń" - tj. akcja zapewnia i loguje transmisję;
   ii. „Blokuj" – tj. akcja blokuje i loguje transmisję;
   iii. „Powiadom" tj. akcja powoduje wyświetlenie powiadomienia, informującego użytkownika o wykrytym zdarzeniu;

30) Moduł musi posiadać funkcjonalność zapewnienia ochrony poprzez kontrolę urządzeń zewnętrznych oraz dostępu do pamięci masowych i zasobów sieciowych połączonych z komputerami.
31) Moduł musi posiadać możliwość monitorowania i blokowania następujących sposobów wymiany / rejestrowania danych:
   d. Urządzeń pamięci masowej: CD/DVD, dysków sieciowych, pamięci masowej USB;
   e. Drukarek.
   f. Klawisza Print Screen.
32) Moduł musi posiadać możliwość nadawania uprawnień kontroli dla urządzeń pamięci masowej takich jak:
   g. Pełny dostęp, w którym dozwolone są operacje: kopiowanie, przenoszenie, otwieranie, zapisywanie, usuwanie oraz wykonywanie plików;
   h. Odczyt, w którym dozwolone są operacje: kopiowanie i otwieranie, zaś niedozwolone są operacje: przenoszenie, zapisywanie, usuwanie oraz wykonywanie plików.
   i. Moduł musi umożliwiać utworzenie listy zatwierdzonych urządzeń pamięci masowej USB tj. kontrola urządzeń musi umożliwiać blokowanie dostępu do wszystkich urządzeń pamięci masowej USB z wyjątkiem tych, które dodano do listy urządzeń zatwierdzonych. Dla tych urządzeń funkcjonalność powinna umożliwiać przyznanie pełnego dostępu lub ograniczyć poziom dostępu.
33) Agent musi posiadać możliwość pracy agenta w trybie offline, bez kontaktu z serwerem zarządzającym.

3.2. Moduł ochrony urządzeń mobilnych (Moduł MDM).

1) Moduł obsługuje systemy operacyjne i zgodność: Android, iOS (iPhone, iPad).
2) Moduł ochrony urządzeń mobilnych (licencje dla 50 urządzeń) musi być w pełni zarządzany z tej samej konsoli zarządzającej, co pozostałe komponenty Systemu OHMS - powinien umożliwiać centralne zarządzanie i monitorowanie stanu zabezpieczeń urządzeń mobilnych.
3) Moduł posiada co najmniej funkcjonalność zaawansowanej ochrony przed zagrożeniami:
   a. Wykrywanie i blokowanie znanych zagrożeń (aplikacje, witryny);
   b. Ochronę przed nieautoryzowanym przesyłaniem danych;
   c. Wykrywanie i usuwanie złośliwego oprogramowania;
   d. Identyfikację podatności w sieciach Wi-Fi;
   e. Wykrywanie i blokowanie złośliwych aplikacji oraz stron internetowych.
   f. Powiadomienia o przestarzałych wersjach systemu operacyjnego.
   g. Mapowanie podatności mobilnych systemów operacyjnych, umożliwiających ocenę ich poziomu bezpieczeństwa.

h. Możliwość wymuszenia szyfrowania danych.

4) Możliwość zdalnej blokady telefonu.
5) Możliwość rejestrowania, aprowizowania i usuwanie urządzeń, a także konfigurowania VPN, Exchange ActiveSync, Wi-Fi.
6) Zbieranie danych telemetrycznych i przekazywanie konsoli zarządczej Systemu OHMS.

3.3. Moduł wykrywania zagrożeń i ochrony sieci - Moduł WZOS

1) Moduł powinien zostać dostarczony w postaci maszyny (maszyn) wirtualnej w środowisku serwerowym, co najmniej jak: VmWare ESXi (wersja 4 i nowsze), KVM oraz Microsoft Hyper-V.
2) Moduł ochrony sieci i rozwiązań teleinformatycznych przed zaawansowanymi atakami typu APT (Advanced Persistent Threat) mającymi na celu uniknięcie wykrycia przez obecne w infrastrukturze zamawiającego systemy zabezpieczające takie jak bramy pocztowe i webowe, systemy IPS/IDS czy oprogramowanie antywirusowe.
3) Rozwiązanie powinno wykrywać szkodliwe obiekty oraz zachowania na każdym etapie ataku. Wykrywanie zagrożeń powinno działać w czasie rzeczywistym. System powinien zapewniać możliwość pracy w trybie OFF-LINE (z wykorzystaniem mirror port-u lub interfejsu TAP).
4) Rozwiązania może się składać z dowolnej (tj. nieograniczonej warunkami licencyjnymi) liczby wirtualnych sond sieciowych o łącznej minimalnej przepustowości 500 Mb/s, z możliwością skalowania do wyższych przepustowości (min. 5000 Mb/s) – bez konieczności wymiany Modułu WZOS.
5) Monitorowanie minimum 10 protokołów sieciowych na pełnym zakresie portów bez potrzeby instalowania dodatkowych elementów systemu.
6) Rozwiązanie powinno móc współpracować z platformą klasy XDR (Extended Detection and Response) oferowanego rozwiązania poprzez dostarczanie zawansowanej telemetrii zdarzeń z monitorowanego ruchu sieciowego minimum w zakresie:
    a. Adresy IP (IPv4, IPv6)
    b. Porty
    c. URL-e
    d. Hasze plików (FileSHA1, FileSHA2)
    e. Domeny
    f. Nazwy plików
    g. Nazwy użytkowników
7) Rozwiązanie musi zapewniać detekcje zagrożeń na podstawie wbudowanych i aktualizowanych przez producenta rozwiązania reguł w okresie wsparcia.
8) Rozwiązanie musi umożliwiać włączenie dostępu SSH, który umożliwi administratorowi zdalne logowanie się w celu zarządzania urządzeniami, wykonywania poleceń oraz kopiowania lub przesyłania plików do urządzenia za pomocą klienta SSH.
9) Rozwiązanie musi udostępniać skrypty demonstracyjne, w celu symulacji ataku i weryfikacji poprawności działania reguł detekcyjnych analizujących ruch z sondy sieciowej.
10) Rozwiązanie musi zapewniać możliwość pobrania plików zidentyfikowanych w telemetrii pochodzącej z sondy sieciowej w postaci skompresowanego i zabezpieczonego hasłem pliku.

4. Moduł bezpiecznego dostępu do sieci (Moduł BDS)

1) Dostawa i wdrożenie niezbędnych licencji dla agentów oraz w celu wykonania redundantnej instalacji Modułu BDS (klastrowanie active-passive), na dwóch serwerach wirtualnych tak, aby zapewnić wysoką niezawodność Modułu BDS. Wszystkie dostarczone licencje muszą być bezterminowe (zachowując w tym czasie pełną funkcjonalność) oraz uprawniać Zamawiającego do uzyskiwania min. 36 miesięcznego wsparcia producenta Modułu BDS np. w celu pobierania aktualizacji usuwających błędy lub wynikających z naturalnego rozwoju Modułu BDS.
2) Moduł BDS ma zawierać wszystkie niezbędne komponenty programowe umożliwiające skonfigurowanie 500 endpointów oraz dalszą rozbudowę w oparciu o rozszerzenie licencji do min. 900 urządzeń podłączonych do sieci lokalnej LAN lub sieci bezprzewodowej WLAN, z uwzględnieniem instalacji agentowej.
3) Wszystkie elementy Modułu BDS powinny być zarządzane centralnie oraz dostarczone jako gotowe maszyny wirtualne (zgodne z min.: Vmware ESXi (wersja 4 i nowsze, KVM i Microsoft Hyper-V), z odpowiednio zabezpieczonym systemem operacyjnym lub jako oprogramowanie instalowane na stacjach roboczych / użytkownika.
4) Wymagane **funkcjonalności podstawowe** Modułu BDS:
    a. Umożliwienie uwierzytelniania użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN dla minimum 500 endpintów z wykorzystaniem:
        i. standardu 802.1X;
        ii. adresu MAC urządzenia;
        iii. formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników Modułu BDS.
    b. Realizacja uwierzytelniania w oparciu o:
        i. wbudowany lub zewnętrzny serwer Radius;
        ii. protokół LDAP;
        iii. wewnętrzną bazę użytkowników i urządzeń.
    c. Realizacja autoryzacji w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS.
    d. Wykonywanie automatycznego wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych - muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci.
    e. Umożliwienie logowania i zapisywania we własnej bazie danych co najmniej następujących informacji:
        i. adresy MAC przełączników, urządzeń końcowych i dostępowych,
        ii. adresy IP ww. urządzeń
        iii. identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe,
        iv. stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów,

v. informacje o użytkownikach,
vi. nazwa użytkownika, do którego przypisany jest urządzenie końcowe,
vii. nazwa zalogowanego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja,
viii. profil/rola jak została przydzielona urządzeniowi końcowemu,
ix. data zarejestrowania urządzenia końcowego w Systemie
x. data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia

f. Umożliwienie tworzenia reguł autoryzacji (kontroli dostępu) opartych o złożone i wielowarunkowe polityki bezpieczeństwa. Powinny one obejmować co najmniej:
i. lokalizację urządzenia w sieci,
ii. przynależność do grupy administracyjnej,
iii. parametr opisujący urządzenie lub użytkownika.

g. Aktywne zapobieganie przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny oraz blokowania.

h. Możliwość powiadamiania poprzez SYSLOG oraz pocztę elektroniczną o sytuacjach krytycznych np. związanych z próbą nieautoryzowanego dostępu do sieci lub awarii wewnętrznych usług Modułu BDS.

i. Wewnętrzna baza urządzeń musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Modułu BDS lub z wykorzystaniem API (bez dodatkowych licencji), Gromadzone dane w bazie urządzeń końcowych są wykorzystywane dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji.

j. Posiadanie bazy minimum 30 kategorii urządzeń końcowych.

k. Realizacja klasyfikacji urządzeń: jednorazowej przy wstępnym uwierzytelnianiu lub rejestracji bądź klasyfikacji wielokrotnej. Klasyfikacja urządzeń i użytkowników musi bazować na harmonogramie z częstotliwością w przedziale od kilku minut do kilku tygodni.

l. Umożliwienie wykonywania na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa.

m. Obsługa telefonów IP wraz z możliwością podłączenia do nich stacji końcowych (przez wbudowany przełącznik w telefonie) przypisując każdemu z urządzeń dedykowane polityki bezpieczeństwa.

n. Autonomiczność w podejmowaniu decyzji o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta – należy założyć, iż obie sytuacje będą miały miejsce jednocześnie w infrastrukturze Zamawiającego.

o. Możliwość przeniesienia urządzenia do kwarantanny w przypadku braku komunikacji z agentem, a także:
i. na urządzeniu podlegającym kwarantannie musi zostać wyświetlona informacja o fakcie przeniesienia urządzenia do kwarantanny oraz informacja

z wytycznymi o działaniach jakie użytkownik urządzenia musi podjąć w celu usunięcia niezgodności;

ii. Administrator Modułu BDS musi mieć możliwość określenia poziomu niezgodności z politykami, po którym będzie następowało przeniesienia urządzenia do kwarantanny.

5) Funkcjonalność w obszarze klasyfikacji urządzeń końcowych z użyciem agenta dedykowanego dla komputerów z systemem Windows i MAC OS X:
   a. Przeprowadzenie następujących testów:
      i. Sprawdzenie wersji agenta;
      ii. Sprawdzenie wersji systemu operacyjnego;
      iii. Sprawdzenie obecności i stanu oprogramowania antywirusowego (niezainstalowany/zainstalowany, uruchomiona ochrona, zaktualizowany);
      iv. Test zapory (włączona/wyłączona);
      v. Test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie);
      vi. Test usługi Windows Update z opcją automatycznego naprawienia niezgodności;
      vii. Test obecności/niewystępowania pliku o określonej nazwie;
      viii. Test obecności procesu (uruchomiony/nieuruchomiony);
      ix. Test rejestru dla systemów Windows (obecność klucza o zdefiniowanej nazwie, typie wartości i wartości, równy bądź różny zadanemu);
      x. Test stanu usługi (uruchomiona/nieuruchomiona);
      xi. Test obecności aplikacji (sprawdzenie czy aplikacja zdefiniowanej nazwie jest zainstalowana).
   b. Przeprowadzanie różnych metod testowania w zależności od lokalizacji urządzenia w sieci, przynależności do grupy administracyjnej, parametru opisującego urządzenie lub użytkownika.
   c. Podczas oceniania urządzenia końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów w przypadku braku zgodności.
6) Moduł BDS musi zapewniać integrację z rozwiązaniami bezpieczeństwa (platformy Firewall, systemy SIEM, systemy Antymalware, systemy MDM) w celu oceny stanu urządzeń końcowych oraz określenia ich zgodności z polityką bezpieczeństwa.
   a. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect" przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci.
   b. W przypadku wykrycia zagrożenia przez system Firewall/SIEM (np. wirus, malware) i przesłania takiej informacji do systemu NAC mogą zostać podjęte następujące akcje automatyczne:
      i. Powiadomienie administratora o zdarzeniu;
      ii. Oznaczenie urządzenia końcowego jako potencjalnie niebezpiecznego „z ryzykiem";
      iii. zablokowanie dostępu do sieci;
      iv. przeniesienie urządzenia do kwarantanny.

c. Po udzieleniu stacji roboczej dostępu do sieci – przekazywana jest do systemu Firewall kontekst użytkownika, który jest zalogowany na tym urządzeniu.

7) Wymagane funkcjonalności w obszarze **profilowania urządzeń odnalezionych w sieci**:
   a. Rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI.
   b. Automatyczne profilowanie urządzeń nieposiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci.
   c. Dodawanie rozpoznanych urządzeń do grup systemowych.
   d. Dla rozpoznanego urządzenia musi być możliwe różnicowanie poziomu dostępu.
   e. Rozpoznawania co najmniej następujących rodzajów urządzeń:
      i. urządzenia z systemem Android, Apple iOS (iPad, iPhone, iPod) oraz MacOS.
      ii. drukarki sieciowe,
      iii. telefony IP,
      iv. stacje robocze z systemami MS Windows, MAC OS, Linux.
      v. kamery IP.

8) Wymagane funkcjonalności w obszarze **logowania, raportowania i alarmowania**:
   a. Udostępnianie danych dla potrzeb audytu (dziennik zdarzeń).
   b. Generowanie szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu / profilu urządzenia końcowego.
   c. Rejestrowanie danych o atrybutach urządzeń końcowych wraz z raportowaniem zmiany w tych atrybutach (np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia).
   d. Gromadzenie i udostępnianie danych historycznych o zmianach stanu konfiguracji portów dostępowych.
   e. Posiadanie centralnej bazy, zawierającej historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy w ramach Modułu BDS.
   f. Możliwość tworzenia własnych szablonów raportów.
   g. Możliwość logowania do zewnętrznych serwerów logów z wykorzystaniem Syslog.
   h. Konfigurowanie generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne (np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora).
   i. Możliwość integracji z modułem analizy i raportowania w celu tworzenia i wykonywania reguł korelujących i alarmujących (rozwiązania typu SIEM).

9) Wymagane funkcjonalności w obszarze **zarządzania Modułem BDS**:
   a. Udostępnianie graficznego interfejsu zarządzania i administracji, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych, dostępny poprzez przeglądarkę internetową.

b. Uwierzytelnianie i autoryzacja dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników lub zewnętrzne repozytorium użytkowników (LDAP lub Radius).
c. Definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania - RBA.
d. Możliwość konfiguracji kont dla co najmniej 3 administratorów Modułu BDS z możliwością określenia praw dostępu do poszczególnych elementów Modułu BDS.

10) Wymagane funkcjonalności w obszarze **zarządzania dostępem gościnnym**:
a. Umożliwienie przyznawania czasowego dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez wypełnienie formularza w portalu rejestracyjnym.
b. Umożliwienie realizacji usług BYOD dla urządzeń prywatnych pracowników.
c. Funkcja portalu rejestracyjnego powinna działać bez udziału lub przy minimalnym udziale pracowników IT; możliwość delegowania uprawnień do akceptowania kont gości przez pracowników nieposiadających uprawnień administracyjnych do Modułu BDS.
d. Wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego.
e. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych.
f. Umożliwienie dopasowania wyglądu portalu logowania gościnnego, w tym co najmniej poprzez zmianę logo strony logowania, zmianę koloru tła i czcionek, treści oraz grafiki.

5. Moduł dwuskładnikowego uwierzytelniania użytkowników (Moduł DUU).

1) Dostawa i wdrożenie niezbędnych licencji dla agentów programowych (software tokens), w celu wykonania redundantnej instalacji Modułu DUU umożliwiającego uwierzytelnianie dla min.: 100 użytkowników i 200 tokenów programowych, obsługę 5 certyfikatów głównych (CA) oraz 500 certyfikatów użytkowników.
2) Dostawa ma obejmować licencje wieczyste dla komponentów Modułu DUU, w tym licencje dla 25 tokenów programowych, umożliwiających uwierzytelnianie dwuskładnikowe oraz upoważniać Zamawiającego do 36 miesięcznego wsparcia producenta w zakresie aktualizacji oprogramowania Modułu DUU.
3) Wszystkie elementy Modułu DUU powinny być zarządzane centralnie oraz dostarczone jako gotowe maszyny wirtualne (zgodne z formatami min.: Vmware ESXi (wersja 4 i nowsze), KVM, Microsoft Hyper-V Server), bez limitów licencyjnych na liczbę procesorów wirtualnych, z odpowiednio zabezpieczonym systemem operacyjnym oraz jako oprogramowanie instalowane na urządzeniach mobilnych użytkownika (*software tokens*).
4) Moduł DUU powinien realizować co najmniej poniższe funkcjonalności ogólne:
a. Zarządzanie w oparciu o interfejs graficzny z wykorzystaniem przeglądarki (protokół HTTPS), bez konieczności stosowania zewnętrznej konsoli zarządzającej oraz poprzez API (dostępne).
b. Możliwość pracy w konfiguracji HA (*High Availability*), z trybem *Active-Passive* lub *Active-Active* w celu zwiększenia niezawodności.
c. Udostępnianie informacji przez Modułu DUU w odpowiedzi na zapytania systemów zewnętrznych, w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż):

i. obciążenia procesor(a/ów);
ii. wykorzystania pamięci;
iii. obciążenia dysku;
iv. zmiany adresu IP interfejsu;
v. informacji o osiąganiu granicznej liczby użytkowników;
vi. informacji o osiąganiu granicznej liczby grup użytkowników;
vii. przekroczeniu liczby uwierzytelnień;
viii. przekroczeniu liczby błędnych uwierzytelnień;
ix. zmiana stanu HA.

d. Graficzną reprezentację statusu uwierzytelnień.
e. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:
   i. Lokalnie w ramach modułu.
   ii. Zdalnie - w oparciu o protokół syslog.
f. Aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego.
g. Tworzenie szyfrowanej kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego:
   i. W oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określeniem godzin i minut.
   ii. Możliwość zapisywania kopii bezpieczeństwa przy pomocy protokołu FTP/SFTP we wskazanej lokalizacji.
h. Możliwość konfiguracji captive portal dla nowo przyłączających się użytkowników.

5) W zakresie funkcji uwierzytelniających, Moduł powinien wspierać nie mniej niż:
   a. Lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania akcji na użytkowniku: tworzenie, przypisanie tokena i zarządzanie nim, blokowanie konta (locking), usuwanie.
   b. Możliwość przechowywania następujących informacji o użytkowniku: nazwa użytkownika, imię/nazwisko, adres email, komórkowego oraz przynajmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników.
   c. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP oraz z pliku CSV.
   d. Integracja z Microsoft Active Directory w celu określania ról i uprawnień użytkowników.
   e. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych), czasu życia hasła oraz możliwości ponownego użycia tych samych haseł.
   f. Konfigurowalną politykę blokowania kont w oparciu o liczbę nieudanych logowa, czas blokowania konta, okres nieaktywności konta, po którym jest blokowane automatycznie.
   g. Możliwość bezpiecznego odzyskiwania haseł np. z wykorzystaniem adresu email.
   h. Funkcjonalność portalu do samodzielnej rejestracji użytkowników:
      i. Tworzenie kont użytkowników może wymagać akceptacji administratora;
      ii. Możliwość tworzenia kont bez ingerencji administratora.
   i. Obsługa protokołu RADIUS zgodną z RFC
      i. Wbudowany serwer RADIUS.
      ii. Konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS.

iii. Integracja z zewnętrznymi serwerami RADIUS.
iv. Możliwość importowania użytkowników RADIUS z zewnętrznego serwera LDAP.

j. Obsługa protokołu TACACS+:
   i. Konfiguracja serwera pozwala na ograniczenie dostępu tylko dla wskazanych klientów.
   ii. Możliwość importowania klientów z pliku CSV oraz przy pomocy API.
   iii. Specyfikowanie listy dozwolonych/blokowanych poleceń powłoki i usług.

k. Obsługa protokołu LDAP:
   i. Wbudowany serwer LDAP.
   ii. Możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).

l. Obsługa SAML - Identity Provider (IdP) proxy

m. Realizacja funkcjonalności SSO (Single Sign On) w oparciu o:
   i. Integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny.
   ii. Dedykowaną aplikację na stacje robocze z systemem Windows
   iii. System RADIUS.
   iv. Informacje uzyskiwane poprzez protokół syslog.
   v. Dedykowany portal.

6) Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe:

a. Możliwość instalacji tokenów programowych (software tokens) dla takich systemów operacyjnych jak Apple iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.

b. Tokeny programowe programowych w systemach iOS i Android realizują:
   i. Aktywację z centralnego systemu uwierzytelniania (*seed provisioning*);
   ii. Możliwość konfiguracji liczby generowanych cyfr w kodzie (co najmniej 6 cyfr);
   iii. Generowanie kodu (cyfr) co konfigurowany czas 30 lub 60 sekund;
   iv. Możliwości dezaktywacji tokena oraz jego reinstalacji tzn. przeniesienia na inne urządzenie mobilne;
   v. Ochronę dostępu poprzez konfigurowalny kod PIN użytkownika;
   vi. Możliwość aktywacji w oparciu o kod QR.
   vii. Możliwość przypisania własnego logotypu organizacji widocznego w aplikacji tokena programowego.

c. Możliwość dostarczenia kodu (wskazania tokena) poprzez:
   i. Aplikację tokena tj. bezpośrednio na urządzenie mobilne.
   ii. Pocztę email - wygaśnięcie kodu w konfigurowalnym czasie 10 sekund – 1h;
   iii. Kanał SMS - wygaśnięcie kodu w konf. czasie 10 sekund – 1h, poprzez konfigurowalną bramkę SMS w oparciu o protokół HTTPS lub bramkę SMTP.

d. W przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem".

e. Możliwość integracji z logowaniem do systemu Windows.

f. Wbudowana możliwość obsługi dla tokenów sprzętowych (hardware):
   i. Realizacja działania w oparciu o protokół OAuth wraz ze wsparciem dla TOTP oraz HOTP.

ii. Tokeny sprzętowe muszą pochodzić od tego samego producenta co system uwierzytelniania i być w ofercie producenta w momencie składania oferty.

7) Moduł powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając co najmniej warunki:
   a. Dla sieci bezprzewodowych wymagane są następujące protokoły: PEAP, EAP-TTLS, EAP-TLS, EAP-GTC;
   b. Wsparcie dla uwierzytelniania w oparciu o adres MAC (*MAC based authentication*).
   c. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach protokołów PEAP, TTL, TLS EAP.
   d. Możliwość samodzielnej rejestracji urządzeń mobilnych przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów.
8) System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, co najmniej w zakresie:
   a. Wsparcia dla własnego, samodzielnego CA (*Certificate Authority*).
   b. Wsparcie dla CA pośredniczącego (*Intermediary CA*).
   c. Ręcznego generowanie certyfikatów z wykorzystaniem interfejsu graficznego.
   d. Możliwości pobrania wygenerowanych certyfikatów.
   e. Możliwości podpisywania certyfikatów z wykorzystaniem protokołu SCEP.
   f. Możliwości automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP.
   g. Możliwość generowania certyfikatów typu wildcard.
   h. Realizacja funkcjonalności CRL (*Certificate Revocation List*).
   i. Wsparcie dla dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).

6. Moduł zarządzania dostępem uprzywilejowanym (Moduł PAM)

Celem wdrożenia Modułu PAM (*Privileged Access Management*) jest ochrona uprzywilejowanych kont przed kradzieżą poświadczeń oraz nadużywaniem uprawnień, poprzez zarządzanie danymi uwierzytelniającymi, kontrolę, monitorowanie oraz audyt uprzywilejowanej aktywności (np. aktywności administratorów sieci, domeny).

1) Moduł PAM powinien być dostarczony jako platforma wirtualna na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania gotowego do uruchomienia w środowisku wirtualizacyjnym (zgodne z rozwiazaniami min.: Vmware ESXi (w wersji 4 i nowszych), KVM i Microsoft Hyper-V) w celu zapewnienia wysokiego poziomu bezpieczeństwa danych i poufności informacji.
2) Dostawa i wdrożenie zestawu niezbędnych bezterminowych licencji pozwalających na podłączenie się co najmniej 5 jednoczesnych użytkowników do nieograniczonej liczby monitorowanych zasobów oraz uprawniających Zamawiającego do aktualizacji przez 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego. Licencje obejmują całość Modułu PAM tj. oprogramowanie wraz z systemami operacyjnymi i innymi komponentami wchodzącymi w skład maszyn wirtualnych i Modułu PAM – w tym funkcje backupu i odtwarzania środowisk serwerowych on-premises.

3) Moduł PAM musi posiadać mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu
4) Wsparcie dla bezpiecznego szyfrowania danych w transmisji i przechowywaniu haseł i kluczy.
5) Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia
6) Moduł PAM musi posiadać przyjazny interfejs graficzny (GUI) umożliwiający przyjazne zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.
7) Musi istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez (Web SFTP, Web SAMBA) oraz SCP.
8) Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH – rozwiązanie musi monitorować komendy wydawane przez operatora sesji.
9) Działanie Modułu PAM musi pozwalać na obsługę połączeń bezpośrednich jak i poprzez serwer pośredniczący (PROXY).
10) Możliwość obsługi niestandardowych protokołów np. poprzez dedykowane wyzwalacze (custom application launcher).
11) Możliwość włączenia ostrzegania użytkowników o nagrywaniu sesji w celu zapewnienia zgodności z wymaganiami RODO.
12) Moduł PAM musi obsługiwać moduł vTPM (Virtual Trusted Platform Module) dla przechowywania kluczy prywatnych użytkowników.
13) Obsługa mechanizmów awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „*glass breaking*”. Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu, w tym musi następować automatycznie nagrywanie obraz podczas wykonywania procedury „*glass breaking*”.
14) Automatyczna zmiana hasła konta po poprawnym zalogowaniu oraz wsparcie dla zaplanowanej zmiany haseł według harmonogramu.
15) Możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów.
16) Ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora, w tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.
17) Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile szyfrowania.
18) Wsparcie dla zaawansowany protokół uwierzytelniania RDP (w tym CredSSP i TLS).
19) Kontrola dostępu oparta na rolach (RBAC), kontrola uprawnień oparta na użytkownikach oraz grupach użytkowników.
20) Kontrola profili dostępowych w formie polityk.
21) Użytkownik uprzywilejowany musi mieć możliwość pracy co najmniej w następujących trybach:
    a. Agentowy – dostępne wszystkie funkcjonalności w ramach Modułu PAM.
    b. Bezagentowo, za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta musi umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji.
    c. Bezagentowo, za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń.
22) Funkcjonalności wymagane w obszarze uwierzytelniania:
    a. Obsługa uwierzytelniania użytkowników za pomocą certyfikatów
    b. Możliwość korzystania z lokalnej bazy danych użytkowników

c. Obsługa uwierzytelniania wieloskładnikowego opartego na SAML
d. Obsługa OIDC (openID Connect), SAML.
e. Obsługa wielu połączeń SAML SP.
f. Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.
g. Wsparcie dla integracji z istniejącymi systemami zarządzania tożsamościami.
h. Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji.
i. Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:
    i. Kontrola dostępu oparta na adresie źródłowym IP użytkownika.
    ii. Ograniczanie dostępu oparte na harmonogramie użytkownika.

23) Możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi, w tym nagrywania i późniejszego odtwarzania sesji.
24) Generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników, co jest celem Modułu PAM.
25) Możliwość integracji z systemami typu IAM i SIEM.
26) Integracja z dostarczanym modułem dwuskładnikowej autentykacji użytkowników – Moduł DUU)
27) Bezpieczne przechowywanie danych uwierzytelniających, takich jak hasła, certyfikaty, klucze prywatne; dane te powinny być zaszyfrowane i chronione przed nieuprawnionym dostępem min algorytmem AES-256.
28) Monitorowanie i kontrola aktywnych sesji, automatyczne wylogowywani nieaktywnych sesji oraz możliwość zdalnego przerwania sesji w przypadku podejrzenia nadużyć.
29) Rejestracja i analiza logów związanych z operacjami wykonywanymi przez konta uprzywilejowane, w celu identyfikacji potencjalnych zagrożeń i śledzenia działań.
30) Wsparcie i pełna konfiguracja z dostarczanym Modułem DUU w celu uzyskania np. możliwości dostępu uprzywilejowanego poprzedzonego logowaniem w oparciu o 2FA.

7. Moduł tworzenia kopii zapasowych dla środowisk serwerowych (Moduł BK).

1) Dostawa i wdrożenie w infrastrukturze IT Zamawiającego min. 8 licencji bezterminowych backupu i odtwarzania środowisk serwerowych on-premises, uprawniających Zamawiającego do 3 lat aktualizacji od Podpisania Protokołu Odbioru Końcowego.
2) Rozwiązanie musi zapewniać możliwość backupu i odtwarzania dla co najmniej 8 środowisk serwerowych w ramach maszyn fizycznych oraz zwirtualizowanych w oparciu o hypervisory: Proxmox VE, VMware vSphere, Microsoft Hyper-V. Dla hypervisora Proxmox VE – wsparcie dla granuralnego odtwarzania poszczególnych plików z maszyn wirtualnych.
3) Rozwiązanie musi umożliwiać integrację z posiadaną przez Zamawiającego konsolą Veeam, za pomocą, której zarządzane są procesy backupu innych zasobów Zamawiającego.
4) Rozwiązanie musi posiadać wbudowane mechanizmy skanowania pozwalające na identyfikację i eliminację zagrożeń malware w trakcie tworzenia kopii zapasowych, chroniąc integralność danych. Możliwość wyszukiwania zaszyfrowanych plików, porównując nowe dane i ostatnią pomyślną kopię zapasową, jeśli została znaleziona. Kopia po procesie porównania musi zostać oznaczona jako jedną z flag: „podejrzana”, „zainfekowana” lub „czysta”.

5) Możliwość strumieniowania logów telemetrycznych (min. kompatybilność z SYSLOG) w celu ich dalszej analizy i informowania o zdarzeniach w ramach dostarczanego i konfigurowanego Systemu NC.
6) Natywne wsparcie dla szyfrowania backupów (AES-256) w trybach szyfrowania: „u źródła", „w czasie transferu", „w stanie spoczynku" oraz wsparcie dla odzyskiwania hasła.
7) Możliwość tworzenia własnych harmonogramów i polityk wykonywania backupu – w tym definiowania okresu retencji danych.
8) Wbudowane mechanizmy tworzenia kopii zapasowych baz danych wykorzystywanych przez Zamawiającego:
    a. Microsoft SQL Server: - wykonywanie kopii w sposób natywny, tj. poprzez mechanizmy API dostarczane przez Microsoft do zarządzania backupami SQL Server; możliwość odtwarzania poszczególnych instancji bazodanowych.
    b. Tworzenie kopii zapasowych i odzyskiwanie baz danych IBM Db2 (środowisko Linux, Intel x64).
9) Możliwość odtwarzania poszczególnych maszyn wirtualnych do pierwotnej lokalizacji lub do nowej lokalizacji, a także odtwarzanie poszczególnych dysków wirtualnych z pełnych backupów oraz migawek.
10) Dostęp do centralnego interfejsu przez przeglądarkę WWW, który umożliwia administratorom monitorowanie i zarządzanie backupami w rozproszonym środowisku:
    a. Monitorowanie, raportowanie i powiadomienia w czasie rzeczywistym dla wielu serwerów backupu;
    b. Uruchamiania i zatrzymywanie procesów backupu i odzyskiwania;
11) Możliwość wykonywania i automatyzacji zadań przy użyciu modułu API oraz poprzez możliwość wykonywania ciągu zadań poprzez skrypty PowerShell.
12) Możliwość wykonywania backupów na urządzenia taśmowe (zgodne z LTO), możliwość obsługi puli nośników w celu uzyskania strategii retencji GFS.

8. Zakres wdrożenia Systemu Nadzoru Cyberbezpieczeństwa

1) Opracowanie harmonogramu wdrożenia Systemów/ Modułów i Licencji oraz zaplanowanie Procedury Odbioru Końcowego Systemu NC.
2) Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej w zakresie zalecanym przez producentów Systemów/ Modułów i Licencji.
3) Przygotowanie dokumentacji projektowej – architektury systemu, wskazania źródeł danych w oparciu o Wykaz systemów i urządzeń Zamawiającego.
4) Przeprowadzenie instalacji wszystkich dostarczonych licencji systemów/modułów zamieszczonych w niniejszym OPZ zgodnie wcześniej przedstawionym i zatwierdzonym harmonogramem realizacji etapów, uzyskanie pełnego działania dostarczonych licencji.
5) Konfiguracja procedury archiwizacji określonych logów źródłowych umożliwiających ich składowanie w infrastrukturze Zamawiającego przez co najmniej 12 miesięcy.
6) Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego Systemu w środowisku Zamawiającego.

7) Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji i będą stanowić załączniki do protokołu odbioru zamówienia.
8) Przeprowadzenie Procedury Odbioru Końcowego Systemu NC zgodnie z wymaganiami z niniejszego dokumentu, udzielenie niezbędnego instruktarzu personelowi IT Zamawiającego odpowiedzialnego za wykonanie odbiorów.
9) Przeprowadzenie przez Wykonawcę analizy powdrożeniowej w zakresie zalecanym przez producentów Systemów/ Modułów i Licencji, plus dodatkowo:
    a. Dokonanie inspekcji konfiguracji urządzeń znajdujących się w środowisku IT Zamawiającego
    b. Porównanie wyników inspekcji z najlepszymi praktykami
    c. Przeprowadzenie tzw. skanu podatności środowiska IT Zamawiającego
    d. Opracowanie Raportu z rekomendacjami.
    e. Asysta i pomoc we wdrożeniu zaleceń umieszczonych w Raporcie
    f. Przekazanie dokumentacji i przeprowadzenie instruktarzu korzystania z konsoli dla personelu IT Zamawiającego
10) Przygotowanie dokumentacji powdrożeniowej zawierającej minimum: opis techniczny środowiska, w tym schemat blokowy systemu wraz z opisem jego składowych oraz przepływu i przetwarzania danych w systemie oraz diagram wdrożenia obejmujący wszystkie składowe systemu wraz ze ścieżkami komunikacji pomiędzy składowymi oraz systemami zewnętrznymi z opisem wykorzystywanych protokołów i portów wszystkich uruchomionych w systemie usług;

8.1. Wykaz systemów i urządzeń Zamawiającego

Środowisko / usługa /urządzenie sieciowe (urządzenia fizyczne oraz zwirtualizowane)	Liczba urządzeń / węzłów będących źródłami logów
Maszyny i środowiska pełniące role lub funkcje serwerowe w tym Active Directory, DNS, DHCP, IIS, WWW, głównie w środowiskach Windows, CentOS, Ubuntu.	min. 50 szt.
Hosty użytkownika tj. komputery, stacje robocze, urządzenia mobilne (iOS, Android) i drukarki sieciowe.	min. 350 szt.
Centralny kontroler WiFi - Ubiqity	1 szt.
Urządzenia centralne – FortiGate, w tym pełniące rolę IDS, IPS, DAM.	4 szt.
Routery w placówkach – FortiGate	16 szt.
Inne routery oraz switche (D-Link, Huawei, Mikrotik, TP-Link)	46 szt.
Serwer VPN – FortiVPN	1 szt.
System zabezpieczania poczty – FortiMail	1 szt.
Inne – Forti Analyser	1 szt.
Inne – Forti Manager	1 szt.
System bezpieczeństwa antywirusowego obejmujący hosty/stacje robocze.	TAK
Rozwiązania VOIP	Nieobjęte wdrożeniem.
System monitoringu wizyjnego	Nieobjęte wdrożeniem.
Liczba unikatowych adresów IP	min. 500 do ustalenia na etapie wdrożenia.

Na etapie analizy przedwdrożeniowej zostaną ustalone szczegółowe zakresy danych przeznaczonych do przetwarzania w Systemie NC, co będzie stanowiło załącznik do dokumentacji powdrożeniowej.

9. Zasady Procedury Odbioru Końcowego Systemu Nadzoru Cyberbezpieczeństwa

Z uwagi na złożoność poszczególnych komponentów Systemu NC oraz interakcję między nimi, Zamawiający wymaga, aby Rezultaty Prac były odebrane na podstawie demonstracji przeprowadzonej dla każdego z modułów Systemu NC oraz współdziałania i reagowania modułów Systemu NC poprzez skonfigurowanie i zaprezentowanie poprawności nadzoru cyberbezpieczeństwa w jednym, centralnym systemie typu SIEM.

9.1. Przygotowanie i konfiguracja logów i formatów wyjściowych

1) Opracowanie harmonogramu uruchomienia systemu SIEM.
2) Przeprowadzenie analizy źródeł danych, przygotowanie propozycji reguł korelacji i raportów, określenie danych kontekstowych w celu demonstracji korelacji i analiz zdarzeń.
3) Określenie, jakie typy logów i alertów mają być wysyłane do SIEM (np. syslog, JSON) z dostarczanych komponentów Systemu NC oraz innych rozwiązań Zamawiającego.
4) Dostosowanie poziomu szczegółowości logów (debug, info, warn, error) do potrzeb analizy bezpieczeństwa i wydajności środowiska.
5) Aktualizacja lub rozbudowa lub ponowna instalacja i konfiguracja systemu SIEM WAZUH.

9.2. Implementacja mechanizmów transportu logów

1) Wybór optymalnego protokołu / metody transportu logów (np.: syslog, CEF, API) oraz skonfigurowanie komponentów Systemu NC - w tym przygotowanie odpowiednich paserów logów lub konfiguracji API w celu przekazywania zdarzeń do systemu SIEM.
2) Zapewnienie prawidłowej łączności z serwerem SIEM poprzez wykonanie niezbędnych konfiguracji sieciowych, weryfikacja i osiągnięcie odpowiednich przepustowości sieci.
3) W razie konieczności - utworzenie odpowiednich reguł dekodera i reguł analitycznych w SIEM dla uzyskiwania danych ze wskazanych źródeł danych, zapewnienie odpowiednich informacji kontekstowych.

9.3. Stworzenie i dostosowywanie reguł korelacji zdarzeń

1) Modyfikacja lub stworzenie schematów i parserów, aby poprawnie kategoryzować zdarzenia (np. alerty bezpieczeństwa, logi systemowe, logi aplikacyjne) z systemów źródłowych.
2) Konfiguracja reguł korelacji zdarzeń pochodzących z różnych źródeł wg. ich znaczenia źródłowego i faktycznego np. wykrycie anomalii w ruchu sieciowym + podejrzana aktywność z konta uprzywilejowanego implikuje informację o możliwym incydencie wysokiego ryzyka.
3) Ustawienie priorytetów i progów alertowania, aby zredukować liczbę fałszywych alarmów, eliminacja znanych fałszywych alarmów poprzez wprowadzenie reguł kategoryzacji.

9.4. Stworzenie pulpitów (dashboard) i raportów w SIEM

1) Dostarczenie i konfiguracja standardowych dashboardów ukazujących kluczowe wskaźniki bezpieczeństwa (np. liczba incydentów, statystyki zagrożeń, aktywność agentów).
2) Przygotowanie dodatkowych 5-ciu spersonalizowanych dashboardów.

3) Przygotowanie raportów cyklicznych (dziennych, tygodniowych, miesięcznych) demonstrujących działanie systemy day-to-day w podziale na grupy odbiorców: kadra zarządzająca i pracownicy działu IT.

9.5. Testowanie przepływu zdarzeń end-to-end.

1) Przekazanie standardowej dokumentacji (High Level Development) i przeprowadzenie instruktarzu korzystania z konsoli dla personelu IT Zamawiającego.
2) Zaproponowanie scenariuszy testowych do akceptacji Zamawiającego - będą stanowić załączniki do protokołu Odbioru Końcowego Systemu NC.
3) Wywołanie wystarczającej liczby kontrolowanych scenariuszy testowych w każdym z systemów źródłowych (np. próbny atak, logowanie uprzywilejowane, naruszenie polityki dostępu do sieci itp) i potwierdzenie, że system SIEM prawidłowo zbiera i parsuje logi źródłowe, koreluje zdarzenia i prezentuje wygenerowane alerty.
4) Wprowadzenie korekty w zakresie zidentyfikowanych problemów – zarówno po stronie systemów źródłowych jak i w przypadku błędnej reprezentacji lub korelacji danych w systemie SIEM.
5) W przypadku problemów dotyczących wydajności Systemu NC (np. na poziomie komunikacji sieciowej modułów Systemu NC, zbytniego obciążenia zasobów sprzętowych poszczególnych komponentów Systemu NC) wprowadzenie niezbędnych poprawek w konfiguracji.
6) Przygotowanie do płynnego przejścia do świadczenia usługi Asysty Powdrożeniowej.

10. Zasady realizacji usługi Asysty Powdrożeniowej

Realizacja usługi Asysty Powdrożeniowej została opisana w Załączniku nr 1 do niniejszego dokumentu.

Załączniki

1) Złącznik nr 1 do OPZ – Zasady realizacji usługi Asysty Powdrożeniowej Systemu Nadzoru Cyberbezpieczeństwa