Cyberbezpieczne Wodociągi

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Załącznik nr 2 do Zapytania ofertowego
pn. „Poprawa cyberbezpieczeństwa
w Zakładzie Usług Gminnych Gminy EłkSp. z o.o.”

Spis treści 2
1. Zakres zamówienia 5
2. OGÓLNE ZASADY RÓWNOWAŻNOŚCI ROZWIĄZAŃ 5
2.1. Zasada ogólna 5
2.2. Szczegółowe kryteria równoważności 6
2.3. Normy, specyfikacje i systemy odniesienia technicznego 7
2.4. Wykazanie równoważności 7
2.5. Przedmiotowe środki dowodowe 8
2.6. Testy odbiorowe a równoważność 8
2.7. Oprogramowanie open source i rozwiązania wielokomponentowe 8
2.8. Wsparcie rozwiązań open source 9
2.9. Kompletność rozwiązania i licencjonowanie 10
2.10. Brak automatycznego uznawania parametrów „wyższych” za równoważne 10
2.11. Integracja z istniejącym środowiskiem Zamawiającego 11
2.12. Odpowiedzialność za integrację 11
2.13. Pierwszeństwo wymagań szczegółowych 11
2.14. Zasada proporcjonalności 12
3. Wymagania wobec przedmiotu zamówienia 12
3.1. Access Point Wi-Fi – S34 – 1 szt. 13
3.2. Oprogramowanie antywirusowe – O01 – 1 kpl 16
3.3. Certyfikaty SSL – O44 – 1 kpl. 21
3.4. Monitoring infrastruktury informatycznej – O33 21
3.5. Centralny menedżer haseł – O32 22
3.6. Szafa RACK – S30 – 1 szt. 24
3.7. Inwentaryzacja aktywów IT/OT/ICS/IIoT – U33 24
3.8. Oprogramowanie DLP – O26 26
3.9. UTM – S07 – 3 szt. 27
3.9.1. Nietechniczne cechy urządzeń 27

3.9.2. Dodatkowe systemy zewnętrzne 28
3.9.3. Wymagania funkcjonalne dla rozwiązań NGFW: 29
3.9.4. Cechy NGFW 29
3.9.5. Silniki detekcyjne i ochronne NGFW 30
3.9.6. Deszyfracja ruchu 32
3.9.7. Obsługa VPN oraz funkcji sieciowych 32
3.9.8. Uwierzytelnienie i ustalanie tożsamości użytkowników 32
3.9.9. Zarządzenie urządzeniami NGFW 33
3.9.10. Interpretacja parametrów wydajnościowych NGFW 33
3.9.11. ZAAWANSOWANA OCHRONA DNS 34
3.9.12. OCHRONA Z WYKORZYSTANIEM MECHANIZMÓW MACHINE LEARNING– 34
3.9.13. WYMAGANIA LICENCYJNE 35
3.10. Testy bezpieczeństwa infrastruktury IT/OT/ICS/IIoT – U02 35
3.11. Urządzenie NAS – S21 – 1 szt. 38
3.12. Serwery fizyczne, w tym HA – S13 – 2 szt. 40
3.13. System operacyjny i licencje dostępowe – O47 47
3.14. Profesjonalne wdrożenie i utrzymanie IT i OT – U09 49
3.14.1. Instalacja i wdrożenie rozwiązań z migracją – 1 szt. 49
3.14.2. System Web Application Firewall (WAF) 64
3.14.3. Oprogramowanie do centralnego zarządzania urządzeniami końcowymi – 1 kpl. 65
3.14.4. System ochrony poczty elektronicznej klasy Email Security 69
3.14.5. Usługa typu Managed Intrusion Detection System (MIDS) IT/OT/ICS 71
3.14.6. Usługa Managed Detection and Response (MDR) 72
3.14.7. Usługa Cyber Threat Intelligence (CTI) IT/OT/ICS/IIoT 74
3.14.8. Świadczenie wsparcia technicznego Systemu do cyberbezpieczeństwa 75
3.15. System SIEM dla obszaru IT i OT – S04 i U39 77
3.15.1. Identity Threat Detection and Response (ITDR) 82
3.15.2. Konfiguracja i uruchomienie funkcjonalności Extended Detection and Response (XDR) w istniejącej platformie SIEM/XDR 83
3.15.3. Wdrożenie warstwy detekcji i reakcji na zagrożenia sieciowe klasy Network Detection and Response (NDR) 85

3.15.4. Licencjonowanie, gwarancja i dokumentacja Systemu SIEM 87
3.16. Oprogramowanie MFA – O43 – 1 licencja 88
3.16.1. Oprogramowanie niezbędne do uruchomienia Systemu 89
3.17. Klucze sprzętowe U2F – S29 90
3.18. Zarządzalny przełącznik sieciowy IT i OT – S27 – 2 szt. 90
3.19. Router OT – O28 92
3.20. Usługi konfiguracji i hardeningu systemów oraz urządzeń IT/OT/ICS/IIoT – U39 95
3.21. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS 97
3.21.1. Przedmiot i cel szkolenia 97
3.21.2. Uczestnicy czas i forma 98
3.21.3. Minimalny program szkolenia 98
3.21.4. Program praktyczny i zasady odbioru szkolenia 99
3.21.5. Materiały dokumentowanie i odbiór 99

1. Zakres zamówienia

Zakres zamówienia obejmuje dostawy i usługi z zadań 3 i 4 projektu oraz szkolenie U28 z zadania 2. Pozycje projektu ujęte w cenie innych dostaw lub usług pozostają obowiązkowe. Wykonawca przekaże matrycę wskazującą dla każdej pozycji rozwiązanie realizujące wymaganie, zakres IT/OT, liczbę urządzeń lub zakres licencji, okres utrzymania i dowód odbioru. Wspólne komponenty mogą realizować kilka pozycji pod warunkiem zapewnienia wszystkich wymaganych funkcji.

2. OGÓLNE ZASADY RÓWNOWAŻNOŚCI ROZWIĄZAŃ

2.1. Zasada ogólna

Opis przedmiotu zamówienia należy interpretować z zachowaniem zasad uczciwej konkurencji, równego traktowania wykonawców, proporcjonalności oraz neutralności technologicznej.
Jeżeli w dokumentacji zamówienia wskazano rozwiązanie referencyjne, znak towarowy, patent, pochodzenie, źródło, producenta, produkt lub szczególny proces w rozumieniu przepisów ustawy Prawo zamówień publicznych, a wskazanie to dotyczy przedmiotu oferowanego przez Wykonawcę, należy je rozumieć jako „lub równoważny", zgodnie z wymaganiami określonymi w dokumentacji postępowania.
Powyższa zasada nie dotyczy nazw produktów i systemów użytych wyłącznie do opisania istniejącej infrastruktury Zamawiającego, środowiska technicznego lub warunków wymaganej integracji.
Za rozwiązanie równoważne uznaje się rozwiązanie, które spełnia wszystkie obligatoryjne wymagania określone dla danej pozycji OPZ, w szczególności wymagania:

- funkcjonalne;
- techniczne;
- wydajnościowe;
- bezpieczeństwa;
- interoperacyjności;
- integracyjne;
- licencyjne;
- eksploatacyjne;
- dotyczące wsparcia i aktualizacji.

Rozwiązanie równoważne nie musi posiadać identycznej:

- architektury wewnętrznej;
- technologii implementacji;
- nazwy modułów;
- bazy danych;
- technologii indeksowania;

- technologii wizualizacji;
- interfejsu użytkownika;
- własnościowego protokołu;
- sposobu realizacji funkcji,

jeżeli zastosowane różnice nie powodują niespełnienia wymagań obligatoryjnych, obniżenia wymaganej wartości użytkowej, poziomu bezpieczeństwa lub interoperacyjności ani powstania po stronie Zamawiającego dodatkowych nieujawnionych kosztów.

Wykonawca sporządzi matrycę zgodności zakresu dostaw i usług z pozycjami zadań 3 i 4 projektu. Dla każdej pozycji, w tym ujętej w cenie innej pozycji, matryca wskaże oferowane rozwiązanie lub usługę, zakres IT/OT, liczbę i lokalizację urządzeń lub zakres licencji, wymagane czynności wdrożeniowe, okres utrzymania oraz dowód wykonania i wynik testu odbiorowego. Wykorzystanie wspólnego rozwiązania do realizacji kilku pozycji jest dopuszczalne pod warunkiem zapewnienia wszystkich wymaganych funkcji i zasobów. Brak oddzielnej wyceny nie oznacza pominięcia pozycji.

2.2. Szczegółowe kryteria równoważności

W przypadku użycia w konkretnej pozycji OPZ produktu lub rozwiązania referencyjnego szczegółowe kryteria równoważności istotne dla tej pozycji powinny wynikać bezpośrednio z jej opisu.

Niniejsza klauzula ogólna nie zastępuje szczegółowego określenia kryteriów równoważności, jeżeli jest ono wymagane dla danego wskazania.

Kryteria mogą obejmować w szczególności:

- wymagane funkcjonalności;
- minimalną wydajność;
- skalowalność;
- obsługiwane protokoły i standardy;
- mechanizmy bezpieczeństwa;
- interoperacyjność;
- sposoby integracji;
- poziom dostępności;
- wymagania dotyczące retencji danych;
- wymagania dotyczące administracji;
- raportowanie;
- aktualizacje;
- wymagany okres wsparcia;
- model licencjonowania;
- wymagane testy funkcjonalne;
- inne parametry wskazane jako obligatoryjne.

O równoważności decyduje spełnienie wymagań określonych przez Zamawiającego oraz osiągnięcie wymaganego rezultatu funkcjonalnego.

Nie wymaga się odwzorowania cech technicznych charakterystycznych wyłącznie dla konkretnego

producenta, jeżeli nie są one konieczne do osiągnięcia celu zamówienia.

2.3. Normy, specyfikacje i systemy odniesienia technicznego

Jeżeli OPZ odwołuje się do:

- norm;
- ocen technicznych;
- specyfikacji technicznych;
- systemów referencji technicznych;

odniesienie takie należy interpretować zgodnie z właściwymi przepisami ustawy Prawo zamówień publicznych.

Przy wskazaniu konkretnej normy, oceny technicznej, specyfikacji technicznej lub systemu odniesienia technicznego należy przyjąć określenie „lub równoważne", jeżeli przepisy wymagają dopuszczenia takiego rozwiązania.

Wykonawca może zaoferować rozwiązanie zgodne z inną normą, oceną techniczną, specyfikacją lub systemem odniesienia, jeżeli wykaże, że zapewnia ono w równoważnym stopniu spełnienie wymagań określonych przez Zamawiającego.

W miarę możliwości określenie „lub równoważna" / „lub równoważne" powinno być zamieszczane również bezpośrednio przy konkretnym odniesieniu występującym w OPZ.

2.4. Wykazanie równoważności

Wykonawca oferujący rozwiązanie równoważne zobowiązany jest wykazać jego zgodność z wymaganiami Zamawiającego na etapie badania i oceny ofert, w zakresie określonym dokumentacją postępowania.

Wykazanie równoważności może następować za pomocą odpowiednich środków dowodowych, w szczególności:

- dokumentacji producenta;
- dokumentacji projektu;
- publicznej dokumentacji technicznej;
- oficjalnego repozytorium projektu;
- dokumentacji API;
- kart katalogowych;
- deklaracji lub certyfikatów;
- raportów z badań;
- raportów testowych;
- innych odpowiednich dokumentów pozwalających potwierdzić określoną funkcjonalność lub parametr.

W przypadku rozwiązań open source dopuszcza się w szczególności wykorzystanie:

- oficjalnej dokumentacji projektu;

- publicznego repozytorium;
- dokumentacji wersji;
- dokumentacji technicznej;
- dokumentacji interfejsów;
- innych publicznie dostępnych materiałów projektu pozwalających wiarygodnie potwierdzić spełnienie wymagania.

Brak komercyjnej karty katalogowej lub dokumentacji producenta nie może sam w sobie stanowić podstawy do odrzucenia rozwiązania open source, jeżeli jego parametry i funkcjonalności mogą zostać wykazane w inny dopuszczalny i wiarygodny sposób.

2.5. Przedmiotowe środki dowodowe

Jeżeli Zamawiający będzie wymagał złożenia przedmiotowych środków dowodowych, ich:

- rodzaj;
- zakres;
- sposób złożenia;
- termin;
- zasady uzupełnienia, o ile są dopuszczalne;

zostaną jednoznacznie określone w dokumentacji postępowania zgodnie z przepisami ustawy Prawo zamówień publicznych.

Wymagane środki dowodowe muszą pozostawać związane z przedmiotem zamówienia oraz być proporcjonalne do przedmiotu i celu zamówienia.

Nie wymaga się przedstawiania dokumentów, które nie są niezbędne do potwierdzenia spełnienia określonego wymagania.

2.6. Testy odbiorowe a równoważność

Testy odbiorowe przeprowadzane po zawarciu umowy służą potwierdzeniu prawidłowej realizacji przedmiotu zamówienia i osiągnięcia wymaganego rezultatu.

Testy odbiorowe nie zastępują obowiązku wykazania równoważności na etapie badania i oceny ofert, jeżeli rozwiązanie zostało zaoferowane jako równoważne.

Wymagania dotyczące testów odbiorowych określone przy poszczególnych pozycjach OPZ stanowią warunki odbioru i realizacji umowy.

2.7. Oprogramowanie open source i rozwiązania wielokomponentowe

Dopuszcza się realizację wymaganych funkcjonalności z wykorzystaniem:

- oprogramowania open source;
- oprogramowania komercyjnego;
- rozwiązania hybrydowego;

- zestawu współpracujących komponentów,

pod warunkiem łącznego spełnienia wszystkich obligatoryjnych wymagań określonych dla danej pozycji OPZ.

Nie wymaga się, aby wszystkie funkcjonalności realizował jeden produkt lub jeden producent, chyba że w konkretnej pozycji OPZ określono inaczej z przyczyn wynikających z wymaganej interoperacyjności, bezpieczeństwa, kompatybilności lub warunków eksploatacji.

Jeżeli oferowane rozwiązanie składa się z kilku komponentów, Wykonawca odpowiada za działanie rozwiązania jako całości, w szczególności za:

- prawidłową instalację;
- konfigurację;
- integrację;
- kompatybilność wersji;
- bezpieczeństwo;
- aktualizacje;
- współdziałanie komponentów;
- diagnozowanie problemów;
- usuwanie problemów wynikających z integracji;
- utrzymanie wymaganej funkcjonalności przez cały wymagany okres wsparcia.

Wykorzystanie kilku komponentów nie może powodować przeniesienia na Zamawiającego odpowiedzialności za ustalanie, który z producentów lub projektów odpowiada za problem dotyczący współdziałania oferowanego rozwiązania.

2.8. Wsparcie rozwiązań open source

Jeżeli dla danej pozycji OPZ nie jest wymagane odpłatne wsparcie producenta lub projektu, dopuszcza się korzystanie z publicznych:

- repozytoriów;
- dokumentacji;
- kanałów dystrybucji;
- baz wiedzy;
- mechanizmów aktualizacji projektu.

W takim przypadku Wykonawca odpowiada w zakresie określonym w OPZ za:

- instalację;
- konfigurację;
- integrację;
- aktualizację;
- diagnostykę;
- usuwanie błędów konfiguracji;
- zapewnienie kompatybilności zastosowanych komponentów;
- wsparcie rozwiązania przez wymagany okres.

Brak komercyjnej subskrypcji producenta lub projektu nie stanowi niespełnienia wymagania, jeżeli dokumentacja konkretnej pozycji OPZ takiej subskrypcji nie wymaga.

2.9. Kompletność rozwiązania i licencjonowanie

Cena oferty musi obejmować wszystkie elementy niezbędne do zachowania wymaganych funkcjonalności przez cały okres wskazany dla danej pozycji OPZ, chyba że dokumentacja wyraźnie wskazuje, że określony element zapewnia Zamawiający.
Dotyczy to w szczególności:

- licencji;
- subskrypcji;
- modułów;
- rozszerzeń;
- konektorów;
- baz sygnatur;
- mechanizmów aktualizacji;
- komponentów programowych;
- wymaganych usług zewnętrznych;
- innych elementów niezbędnych do spełnienia obligatoryjnych wymagań.

Oferowane rozwiązanie nie może wymagać w okresie obowiązywania umowy lub wymaganego okresu wsparcia zakupu przez Zamawiającego dodatkowego elementu niewskazanego w ofercie, jeżeli bez niego rozwiązanie przestaje spełniać obligatoryjne wymagania OPZ.
Jeżeli po upływie okresu objętego zamówieniem określona funkcjonalność wymaga dalszej odpłatnej subskrypcji lub licencji, fakt ten powinien zostać jednoznacznie wskazany w ofercie, jeżeli informacja taka jest wymagana przez dokumentację postępowania.

2.10. Brak automatycznego uznawania parametrów „wyższych” za równoważne

Samo zaoferowanie parametru liczbowo wyższego lub szerszego zakresu funkcji nie oznacza automatycznie spełnienia wymagań równoważności.
Ocenie podlega całokształt wymagań określonych dla danej pozycji, w tym wpływ rozwiązania na:

- bezpieczeństwo;
- interoperacyjność;
- wydajność;
- kompatybilność;
- ochronę danych;
- koszty eksploatacji;
- sposób zarządzania;
- istniejącą architekturę Zamawiającego.

Parametr odmienny od wskazanego może zostać uznany za równoważny, jeżeli spełnia wymagania

minimalne i nie powoduje pogorszenia cech istotnych z punktu widzenia celu zamówienia.

2.11. Integracja z istniejącym środowiskiem Zamawiającego

Nazwy produktów, producentów lub technologii występujące w OPZ jako opis już posiadanego lub eksploatowanego środowiska Zamawiającego służą określeniu:

- stanu istniejącego;
- wymaganego zakresu kompatybilności;
- warunków interoperacyjności;
- zakresu integracji;
- uwarunkowań technicznych realizacji.

Takie wskazanie nie oznacza samo przez się obowiązku zaoferowania przez Wykonawcę produktu tego samego producenta.

Jeżeli prawidłową integrację można osiągnąć za pomocą udokumentowanego i wspieranego mechanizmu interoperacyjności, dopuszcza się jego wykorzystanie zgodnie z wymaganiami konkretnej pozycji OPZ.

2.12. Odpowiedzialność za integrację

Jeżeli spełnienie wymagania wymaga integracji kilku oferowanych komponentów, Wykonawca odpowiada za jej prawidłowe wykonanie oraz utrzymanie w okresie wymaganym dla danej pozycji.

W szczególności odpowiedzialność ta obejmuje:

- konfigurację interfejsów;
- mapowanie wymaganych danych;
- kompatybilność wersji;
- uwierzytelnianie;
- szyfrowanie transmisji, jeżeli jest wymagane;
- aktualizację konfiguracji po aktualizacji komponentów;
- diagnostykę błędów integracji.

2.13. Pierwszeństwo wymagań szczegółowych

Niniejsze zasady mają charakter ogólny i obowiązują wszystkie części OPZ, o ile opis konkretnej pozycji nie przewiduje wymagań bardziej szczegółowych.

Jeżeli dla konkretnej pozycji określono szczegółowo:

- kryteria równoważności;
- wymagania minimalne;
- wymagania integracyjne;
- wymagania licencyjne;

- środki dowodowe;
- testy odbiorowe;
- okres wsparcia;
- sposób realizacji;

należy stosować je łącznie z niniejszymi zasadami.

W przypadku rozbieżności pierwszeństwo mają wymagania szczegółowe właściwe dla danej pozycji OPZ, z zastrzeżeniem bezwzględnie obowiązujących przepisów prawa.

2.14. Zasada proporcjonalności

Wymagania dotyczące równoważności, dokumentowania funkcjonalności, integracji oraz przedmiotowych środków dowodowych należy interpretować w sposób proporcjonalny do:

- charakteru danej pozycji;
- jej wartości;
- znaczenia dla bezpieczeństwa;
- ryzyka technicznego;
- zakresu wymaganej integracji.

Nie wymaga się od Wykonawcy przedstawiania informacji lub dokumentów, które nie są niezbędne do obiektywnego potwierdzenia spełnienia danego wymagania.

3. Wymagania wobec przedmiotu zamówienia

Lp.	Minimalne wymagania
1.	a) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej i muszą być wyprodukowane po 1 stycznia 2026 r. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. b) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. c) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta. d) W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. e) Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

	f) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta. g) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownikowi w języku polskim lub angielskim w formie papierowej lub elektronicznej. h) Gwarancja i serwis na urządzenia musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku gdy Oferent nie posiada takiej autoryzacji. i) Urządzenia na etapie dostawy Producent => Zamawiający nie mogą podlegać modyfikacjom. j) Zamawiający wymaga możliwości sprawdzenia statusu gwarancji i konfiguracji oferowanego sprzętu na stronie producenta po podaniu jego numeru seryjnego, strona producenta musi być podstroną głównej domeny producenta sprzętu. k) Na min. 3 dni przed dostawą sprzętu należy przesłać Zamawiającemu wykaz numerów seryjnych oferowanych urządzeń celem weryfikacji u producenta. l) Wymagana ogólnopolska, telefoniczna infolinia/linia techniczna producenta w języku polskim (ogólnopolski numer o zredukowanej odpłatności 0-800 lub 0-801).

3.1. Access Point Wi-Fi – S34 – 1 szt.

Urządzenie musi spełniać co najmniej poniższe wymagania:
1. Typ urządzenia: urządzenie sieciowe – dwuradiowy punkt dostępowy, wykonany w zamkniętej obudowie, przeznaczony do montażu na ścianie, suficie podwieszanym lub suficie trwałym, z możliwością zastosowania dodatkowych akcesoriów montażowych.
2. Kompatybilność: urządzenie musi być w 100% kompatybilne z wyspecyfikowanym kontrolerem sieci bezprzewodowej.
3. Interfejsy przewodowe:
3.1. Porty Ethernet: minimum 2 × 10/100/1000Base-T.
3.2. Port konsolowy: minimum 1 port szeregowy konsoli z interfejsem RJ-45.
3.3. Port USB: minimum 1 × USB 2.0.
4. Warunki pracy: temperatura pracy w zakresie co najmniej od 0°C do 50°C.
5. Montaż: możliwość montażu naściennego oraz sufitowego.
6. Zasilanie:
6.1. Złącze zasilania: 12 V DC.
6.2. Power over Ethernet: obsługa zasilania zgodnego z IEEE 802.3af/at.
6.3. Zasilacz zewnętrzny: możliwość zasilania za pomocą zewnętrznego adaptera o napięciu wejściowym 100–240 V AC i napięciu wyjściowym 12 V DC.

6.4. Pobór mocy: nie większy niż 13 W.
7. Tryby pracy: możliwość pracy zarówno w trybie zarządzanym przez kontroler (FIT), jak i w trybie samodzielnym (FAT).
8. Wydajność: sumaryczna prędkość przesyłania danych nie mniejsza niż 1,775 Gb/s.
9. Pasma częstotliwości: równoczesna praca w pasmach 2,4 GHz oraz 5 GHz.
10. MIMO: obsługa komunikacji bezprzewodowej minimum 2×2:2 MIMO.
11. Anteny:
11.1. Pasmo 2,4 GHz: wbudowane anteny o zysku minimum 4 dBi.
11.2. Pasmo 5 GHz: wbudowane anteny o zysku minimum 5 dBi.
12. Moc nadawcza: moc wyjściowa na złączu antenowym:
12.1. Pasmo 2,4 GHz: minimum 23 dBm.
12.2. Pasmo 5 GHz: minimum 23 dBm.
13. Regulacja mocy: możliwość regulacji mocy nadawczej z krokiem nie większym niż 1 dBm.
14. Wymagane standardy i częstotliwości pracy radia:
14.1. IEEE 802.11a/n/ac: zakres częstotliwości 5,150–5,850 GHz.
14.2. IEEE 802.11b/g/n/ax: zakres częstotliwości 2,400–2,483 GHz.
14.3. IEEE 802.11ax: obsługa zakresów 5,150–5,250 GHz, 5,250–5,350 GHz oraz 5,725–5,850 GHz.
15. Obsługiwane technologie modulacji:
15.1. IEEE 802.11b: BPSK, QPSK, CCK.
15.2. IEEE 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM.
15.3. IEEE 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.
15.4. IEEE 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.
16. Stopień ochrony: minimum IP41.
17. Wirtualne punkty dostępowe: obsługa minimum 32 jednoczesnych wirtualnych punktów dostępowych (BSSID).
18. Strumienie przestrzenne: obsługa minimum 2 strumieni przestrzennych.
19. Funkcje łączności bezprzewodowej: urządzenie musi obsługiwać co najmniej: DCA – dynamiczne dostosowanie kanałów, TPC – kontrolę mocy nadawania, wykrywanie martwych obszarów, ukrywanie SSID, RTS/CTS, skanowanie środowiska radiowego, limitowanie liczby użytkowników, eliminację terminali ze zbyt słabym sygnałem, wymuszanie roamingu terminali o słabym sygnale, inteligentną kontrolę terminali w oparciu o równomierne rozłożenie czasu transmisji oraz okresowe włączanie i wyłączanie SSID.
20. Funkcje bezpieczeństwa: urządzenie musi obsługiwać co najmniej: szyfrowanie 64/128-bit WEP, TKIP i CCMP, IEEE 802.11i, WAPI, autentykację na podstawie adresu MAC, autentykację LDAP, autentykację PEAP, WIDS/WIPS, ochronę widma w czasie rzeczywistym, zabezpieczenie przed atakami typu DoS, filtrowanie ramek, białą listę, statyczną i dynamiczną czarną listę, izolowanie stacji bezprzewodowych, SAVI, izolację użytkownika, listy kontroli dostępu (ACL), kontrolę dostępu do wolnych zasobów oraz kontrolę dostępu terminali bezprzewodowych.
20.1. Praca awaryjna: urządzenie musi zapewniać bezprzerwową pracę w przypadku utraty połączenia z kontrolerem.

20.2. Automatyczne wyłączanie usług: możliwość automatycznego wyłączania usług w przypadku przekroczenia zakładanego czasu dostępności usługi.
20.3. Punkt dostępowy musi obsługiwać WPA3-Enterprise oraz uwierzytelnianie IEEE 802.1X z wykorzystaniem usługi RADIUS. Wykonawca uruchomi sieć służbową z uwierzytelnianiem 802.1X, odseparowaną od sieci gościnnej i odpowiednio przypisaną do VLAN. W ramach odbioru zostanie zweryfikowane poprawne uwierzytelnienie użytkownika lub urządzenia oraz odrzucenie dostępu bez wymaganych uprawnień.
20.4. W konfiguracji produkcyjnej nie dopuszcza się stosowania WEP ani TKIP. Sieć służbowa zostanie uruchomiona z WPA3-Enterprise oraz uwierzytelnianiem IEEE 802.1X.
21. Funkcje sieciowe: obsługa statycznego adresu IP, klienta DHCP, pakietów IPv6, IGMP Snooping, roamingu pomiędzy punktami dostępowymi AP, roamingu pomiędzy kontrolerami AC, WDS oraz kontroli dostępu do punktów dostępowych.
22. Funkcje QoS: urządzenie musi obsługiwać co najmniej:
22.1. IEEE 802.11e (WMM).
22.2. Mapowanie VLAN i SSID: możliwość mapowania różnych sieci VLAN oraz SSID do różnych polityk QoS.
22.3. Mapowanie strumieni danych: możliwość mapowania różnych strumieni danych, na podstawie różnych pól pakietów, do różnych polityk QoS.
22.4. Load balancing: równoważenie obciążenia w oparciu o liczbę użytkowników, ilość ruchu lub zakres częstotliwości.
22.5. Ograniczanie przepustowości: możliwość definiowania limitów przepustowości dla AP, SSID, terminali oraz strumieni danych.
22.6. Oszczędzanie energii: obsługa trybu oszczędzania energii.
22.7. Odzyskiwanie komunikacji: automatyczne odzyskiwanie komunikacji z kontrolerem AC.
22.8. Identyfikacja terminali: inteligentne identyfikowanie terminali.
22.9. Preferowanie pasma 5 GHz: urządzenie musi umożliwiać początkową inicjalizację połączenia w paśmie 5 GHz dla urządzeń końcowych obsługujących jednocześnie pasma 2,4 GHz oraz 5 GHz.
23. Zarządzanie: urządzenie musi obsługiwać co najmniej:
23.1. Zarządzanie centralne: poprzez kontroler sieci bezprzewodowej (AC).
23.2. Rejestrowanie zdarzeń: lokalny log, syslog oraz eksport plików logów.
23.3. AP Escape: w przypadku braku komunikacji z którymkolwiek z kontrolerów AC punkty dostępowe muszą umożliwiać dalszą pracę jako niezależne urządzenia, z zachowaniem obsługi zarówno aktualnie podłączonych, jak i nowych użytkowników.
23.4. Watchdog: sprzętowy watchdog.
23.5. Zdalna autentykacja: możliwość zdalnej autentykacji punktu dostępowego do kontrolera AC poprzez sieć warstwy L3 oraz Internet, przy kontrolerze AC posiadającym publiczny adres IP, bez konieczności wykorzystywania tuneli VPN.
24. Gwarancja: gwarancja typu lifetime, obowiązująca dodatkowo przez minimum 1 rok od wycofania produktu z linii produkcyjnej. W przypadku wycofania produktu z linii produkcyjnej wcześniej niż 5 lat od daty zakupu, gwarancja musi obowiązywać przez minimum 6 lat od daty zakupu.

3.2. Oprogramowanie antywirusowe – O01 – 1 kpl.

Ochrona obejmie stacje robocze i serwery IT oraz hosty OT wskazane w wykazie chronionych zasobów. Dla hostów OT Wykonawca zapewni funkcjonalności EDR wymagane w projekcie, realizowane przez system ochrony endpointów lub współdziałające komponenty SIEM/XDR. Instalacja agentów i konfiguracja reakcji muszą uwzględniać zgodność z oprogramowaniem HMI/SCADA oraz zalecenia producentów. Automatyczne izolowanie hostów OT lub blokowanie procesów technologicznych wymaga zatwierdzonej procedury. Odbiór obejmie sprawdzenie telemetrii, detekcji testowego zdarzenia i uzgodnionego mechanizmu reakcji.

1. Ilość licencji: system musi umożliwić bezproblemową i stabilną obsługę na co najmniej 20 urządzeniach jednocześnie.
2. Ochrona antywirusowa i antyspyware

2.1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

2.2. Interfejs oraz pomoc techniczna świadczona w języku polskim.

2.3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.

2.4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor itp.

2.5. Wbudowana technologia do ochrony przed rootkitami.

2.6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

2.7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.

2.8. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

2.9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszającym obciążenie systemu w trakcie wykonywania tego procesu.

2.10. Możliwość skanowania dysków sieciowych i dysków przenośnych.

2.11. Skanowanie plików spakowanych i skompresowanych.

2.12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.

2.13. Możliwość dodawania wykluczeń na podstawie:

- pliku,
- folderu,
- rozszerzenia,
- procesu,
- hasha pliku,
- hasha certyfikatu,
- nazwy zagrożenia,
- wiersza poleceń,

- IP/maski.

2.14. Skanowanie poczty opartej o protokoły IMAP, MAPI, POP3 i SMTP w czasie rzeczywistym.
2.15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.
2.16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
2.17. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS.
2.18. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
2.19. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
2.20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
2.21. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
2.22. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
2.23. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
2.24. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
2.25. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
2.26. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
2.27. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
2.28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
2.29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
2.30. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
2.31. Wbudowany IDS.
2.32. Możliwość tworzenia list sieci zaufanych.
2.33. Możliwość dezaktywacji funkcji zapory sieciowej.
2.34. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
2.35. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań, konfigurowalne w politykach bezpieczeństwa.
2.36. Komunikacja między konsolą zarządzającą a punktami końcowymi jest szyfrowana.
2.37. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia

exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

- możliwość wymuszenia funkcji DEP systemu Windows,
- możliwość wymuszenia relokacji modułów (ASLR) dla Windows.

2.38. Ochrona przed atakami sieciowymi – mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

- pierwszy dostęp,
- dostęp do poświadczeń,
- wykrycie,
- Crimeware,
- ruch boczny.

2.39. Ochrona przed ransomware – możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego, czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach:
3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4.

2.40. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows.

2.41. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.

2.42. System musi umożliwiać skanowanie oprogramowania układowego UEFI.

2.43. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.

2.44. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej.

2.45. Telemetria – możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i Linux do serwera Syslog (JSON).

2.46. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).

3. Stacje robocze i serwery

3.1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

3.2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor itp.

3.3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.

3.4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.

3.5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora; przy próbie deinstalacji program powinien pytać o hasło.
3.6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
3.7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
3.8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
3.9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
3.10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
3.11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie", możliwość wyświetlenia danych do pomocy technicznej tj.: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux.
3.12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
4. Konsola zdalnej administracji
4.1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
4.2. Możliwość integracji wielu domen Active Directory.
4.3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4.4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego: aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki.
4.5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
4.6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
4.7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
4.8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
4.9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
4.10. Możliwość ręcznego, na żądanie, i automatycznego generowania raportów według ustalonego harmonogramu oraz wyeksportowania ich do formatu PDF i CSV. Również zbiorczo w formie archiwum ZIP.
4.11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
4.12. Możliwość generowania raportu co godzinę.
4.13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
4.14. Możliwość dodania etykiety do stacji roboczej.
4.15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji

zdalnej.

4.16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.

4.17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.

4.18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.

4.19. Wsparcie techniczne mailowe i telefoniczne w języku polskim od poniedziałku do piątku w godzinach 8:00–16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem 24/7 w języku angielskim.

4.20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego, jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.

4.21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:

- zakresu adresów IP/IP,
- adresu bramy,
- adresu serwera WINS,
- adresu serwera DNS,
- połączenia DHCP sufiksów DNS,
- możliwości rozwiązania hosta przez punkt końcowy,
- typu sieci,
- nazwy hosta.

4.22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC 6238.

4.23. Możliwość naprawy instalacji agenta z poziomu konsoli.

4.24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.

4.25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.

4.26. Możliwość wyświetlenia, czy punkt końcowy jest serwerem czy stacją roboczą.

4.27. Możliwość wyświetlenia informacji, czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub macOS.

4.28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.

4.29. Menu tworzenia paczek instalacyjnych musi określać, czy dany moduł jest dostępny dla stacji roboczych Windows, serwerów Windows, Linux, macOS.

4.30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów macOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.

4.31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli

administracyjnej.
4.32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
4.33. Zdarzenia z modułów mogą być przesyłane do Syslog (JSON, CEF).
4.34. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.
4.35. Możliwość aktualizacji serwera administracyjnego bez potrzeby jego ponownej instalacji.
4.36. Możliwość określenia własnego serwera NTP.
4.37. Integracja z vCenter Server.
4.38. Integracja z Xen Server.
4.39. Możliwość przechowywania plików poddanych kwarantannie na scentralizowanym udziale sieciowym.
4.40. System umożliwia zezwolenie na dostęp do konsoli zarządzającej dla użytkowników Active Directory z grupy Security Groups.
4.41. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

- pakiety,
- konta,
- sieć,
- kwarantanna,
- raporty,
- polityki.

3.3. Certyfikaty SSL – O44 – 1 kpl.

1. Wykonawca zapewni publicznie zaufane certyfikaty TLS dla domen/FQDN wskazanych przez Zamawiającego.
2. Certyfikaty muszą być zgodne z X.509 v3 i współpracować z aktualnymi popularnymi przeglądarkami oraz systemami operacyjnymi.
3. Obsługiwane muszą być co najmniej klucze RSA 2048 bit lub silniejsze oraz ECDSA P-256 lub silniejsze, z algorytmem skrótu co najmniej SHA-256 lub równoważnym.
4. Jeżeli mechanizm CA to obsługuje, dostępna musi być weryfikacja statusu certyfikatu przez OCSP i/lub CRL.
5. Dopuszcza się certyfikaty SAN i Wildcard, jeżeli wynika to z wykazu systemów Zamawiającego.
6. Wykonawca zapewni ciągłość ważności certyfikatów przez 36 miesięcy, w tym wszystkie niezbędne odnowienia i ponowne wystawienia.

3.4. Monitoring infrastruktury informatycznej – O33

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie systemu monitorowania infrastruktury informatycznej Zamawiającego, wyposażonego w interfejs graficzny umożliwiający bieżące śledzenie stanu urządzeń i usług oraz reagowanie na występujące

nieprawidłowości.
System musi obejmować infrastrukturę IT i OT objętą projektem, w szczególności:

1. Serwery fizyczne i wirtualne.
2. Usługi i środowiska wirtualizacyjne.
3. Zasoby dyskowe i urządzenia NAS.
4. Systemy wykonywania kopii zapasowych.
5. Urządzenia sieciowe, w tym przełączniki, routery i UTM/NGFW.
6. Drukarki i inne urządzenia sieciowe wskazane przez Zamawiającego.
7. Dostępne interfejsy diagnostyczne systemów OT, w zakresie pozwalającym na bezpieczne monitorowanie infrastruktury przemysłowej.

Wymagania funkcjonalne:
1. System musi umożliwiać monitorowanie dostępności urządzeń i usług.
2. System musi umożliwiać monitorowanie wykorzystania zasobów, w szczególności obciążenia procesorów, pamięci operacyjnej, przestrzeni dyskowej i interfejsów sieciowych, w zakresie udostępnianym przez monitorowane urządzenia.
3. System musi umożliwiać monitorowanie stanu usług systemowych oraz mechanizmów wykonywania kopii zapasowych.
4. System musi umożliwiać definiowanie progów alarmowych dla monitorowanych parametrów.
5. System musi automatycznie generować powiadomienia o niedostępności urządzeń, awariach usług oraz przekroczeniach ustalonych progów alarmowych.
6. System musi posiadać interfejs graficzny umożliwiający prezentację stanu monitorowanych urządzeń i usług oraz przygotowanie dashboardów.
7. System musi umożliwiać przeglądanie informacji o monitorowanych zasobach i występujących zdarzeniach.

Pozostałe wymagania:
1. Wykonawca zainstaluje i skonfiguruje system monitorowania infrastruktury objętej zamówieniem.
2. Wykonawca skonfiguruje pozyskiwanie danych z monitorowanych urządzeń z wykorzystaniem dostępnych, udokumentowanych interfejsów i protokołów.
3. Wykonawca skonfiguruje progi alarmowe, powiadomienia oraz dashboardy.
4. Monitorowanie infrastruktury OT musi odbywać się metodami niezakłócającymi procesów technologicznych.
5. Wykonawca zapewni integrację systemu monitorowania z pozostałymi rozwiązaniami bezpieczeństwa w zakresie wymaganym przyjętą architekturą IT/OT.

3.5. Centralny menedżer haseł – O32

1. Typ rozwiązania: lokalny (self-hosted), szyfrowany menedżer haseł przeznaczony do obsługi indywidualnych sejfów użytkowników, instalowany w infrastrukturze Zamawiającego. Dane sejfów nie mogą wymagać przechowywania w chmurze producenta.
2. Licencjonowanie: rozwiązanie musi umożliwiać obsługę minimum 15 niezależnych kont użytkowników bez konieczności zakupu płatnego planu biznesowego lub cyklicznych licencji per użytkownik. Dopuszcza się oprogramowanie bezpłatne i open source, wykorzystywane zgodnie z warunkami licencyjnymi producenta/projektu.

3. Wdrożenie: rozwiązanie musi być przeznaczone do zastosowań produkcyjnych i umożliwiać pracę w środowisku wirtualnym Zamawiającego, w szczególności VMware, Hyper-V, OpenStack lub równoważnym. Komponenty aplikacyjne muszą pochodzić z oficjalnych źródeł producenta/projektu.
4. Praca bez dostępu do Internetu: podstawowe funkcje systemu nie mogą wymagać bezpośredniego dostępu serwera do Internetu. Musi istnieć możliwość instalacji i aktualizacji offline poprzez kontrolowane dostarczenie wymaganych pakietów, plików lub obrazów kontenerowych.
5. Sejfy użytkowników: każdy użytkownik musi posiadać własne konto i indywidualny szyfrowany sejf umożliwiający przechowywanie co najmniej loginów, haseł, bezpiecznych notatek, kart, tożsamości, URI/URL oraz pól niestandardowych. Użytkownik musi mieć możliwość organizowania wpisów w folderach.
6. Bezpieczeństwo danych: dane sejfu muszą być szyfrowane po stronie klienta przed przesłaniem na serwer zgodnie z modelem zero-knowledge. Wymagane jest szyfrowanie o sile co najmniej AES-256 lub równoważnej oraz funkcja KDF obsługująca co najmniej PBKDF2-SHA256 lub Argon2id.
7. Uwierzytelnianie: system musi umożliwiać każdemu użytkownikowi samodzielne skonfigurowanie 2FA za pomocą TOTP oraz FIDO2/WebAuthn z wykorzystaniem sprzętowego klucza bezpieczeństwa, np. YubiKey lub równoważnego.
8. Funkcje użytkownika: system musi zapewniać generator haseł i passphrase, automatyczne wypełnianie danych logowania, powiązanie wpisów z URI/domeną, konfigurowalne czyszczenie schowka oraz historię poprzednich haseł.
9. Import i eksport: wymagany jest import danych co najmniej z formatów CSV i JSON oraz eksport co najmniej do CSV, JSON i zaszyfrowanego formatu JSON. Eksport szyfrowany musi nadawać się do wykorzystania w procesie migracji lub odtworzenia zgodnie z dokumentacją producenta.
10. Klienci: wymagane są oficjalne klienty producenta dla co najmniej Windows, macOS, Linux, iOS i Android oraz rozszerzenia dla Chrome/Chromium, Firefox, Edge i Safari. Wymagany jest również interfejs webowy i narzędzie CLI. Klienci muszą umożliwiać wskazanie własnego adresu URL/FQDN lokalnej instancji.
11. Synchronizacja: dane sejfu muszą synchronizować się pomiędzy klientami użytkownika po połączeniu z lokalnym serwerem. Wcześniej zsynchronizowane dane muszą być dostępne w trybie offline co najmniej do odczytu.
12. Komunikacja: połączenia klient–serwer muszą wykorzystywać HTTPS/TLS. System musi umożliwiać zastosowanie certyfikatu dostarczonego przez Zamawiającego, w tym certyfikatu wydanego przez wewnętrzne CA, oraz wykorzystanie lokalnej nazwy DNS/FQDN.
13. Administracja: administrator lokalnej instancji musi mieć możliwość co najmniej przeglądania i usuwania zarejestrowanych kont użytkowników oraz wyłączenia otwartej rejestracji nowych kont, bez możliwości odszyfrowania zawartości indywidualnych sejfów.
14. Kopie zapasowe: system musi umożliwiać wykonanie kopii zapasowej danych wymaganych do odtworzenia instancji, w szczególności bazy danych, konfiguracji i certyfikatów. Użytkownik musi dodatkowo mieć możliwość wykonania szyfrowanego eksportu własnego sejfu.
15. Logowanie i monitoring: rozwiązanie musi generować logi techniczne i operacyjne umożliwiające diagnostykę oraz pozwalać na ich przekazywanie do systemu SIEM/Wazuh za pośrednictwem systemu

operacyjnego, reverse proxy, syslog, platformy kontenerowej lub agenta SIEM.
16. Dostęp do systemu: lokalna instancja powinna być dostępna z sieci LAN oraz poprzez kontrolowany VPN. Dostęp administracyjny musi być możliwy do ograniczenia do dedykowanej sieci/VLAN administracyjnego.
17. Bezpieczeństwo eksploatacyjne: system musi umożliwiać automatyczne blokowanie sejfu po okresie bezczynności. Dla wskazanych administratorów i użytkowników należy skonfigurować MFA FIDO2/WebAuthn.
18. Poświadczenia krytyczne: poświadczenia do systemów krytycznych, w szczególności OT/SCADA, urządzeń sieciowych, UTM, systemów backupu oraz kont break-glass, nie mogą być przechowywane wyłącznie w indywidualnym sejfie jednego użytkownika.
19. Aktualizacje: rozwiązanie musi umożliwiać aktualizację do nowszych wersji udostępnianych przez producenta/projekt bez konieczności zakupu dodatkowej płatnej licencji w zakresie funkcji objętych oferowanym wariantem.
20. Wysoka dostępność: nie wymaga się klastra HA. Dostępność usługi może być zapewniona przez platformę wirtualizacyjną, monitoring, kopie zapasowe oraz procedurę odtworzeniową.

3.6. Szafa RACK – S30 – 1 szt.

1.Rozmiar: 32U.
2.Wymiary: 600 x 1000 mm.
3.Nośność statyczna: 800 kg.
4.Wyposażenie: 2szt listwa zasilająca 6 gniazd, 1,8m kabel zasilający, 2x półka, panel 2ch wentylatorów z termostatem, 24 portowy pathpanel UTP kat. 6.
5.Drzwi przednie perforowane lub szklane, zamykane na zamek, montaż prawostronny i lewostronny.
6.Drzwi boczne zatrzaskowe (możliwość demontażu).
7.Drzwi tylne pełne stalowe lub perforowane zamykane na klucz.
8.Kółka z hamulcem.
9.Regulowane nóżki.
10. Otwory na przewody: 3 przepusty kablowe w podłodze i w suficie.
11.Otwory wentylacyjne.
12. Gwarancja min. 24 m-ce.

3.7. Inwentaryzacja aktywów IT/OT/ICS/IIoT – U33

1. Przedmiot i zakres usługi
1.1. Przedmiotem zamówienia jest wykonanie inwentaryzacji zasobów teleinformatycznych i przemysłowych Zamawiającego objętych projektem.
1.2. Inwentaryzacja musi obejmować infrastrukturę IT oraz OT/ICS/IIoT, w szczególności:
a) serwery fizyczne i wirtualne;

b) stacje robocze;
c) urządzenia sieciowe, w tym routery, przełączniki i urządzenia UTM/NGFW;
d) urządzenia pamięci masowej i systemy backupu;
e) systemy operacyjne i oprogramowanie;
f) systemy bezpieczeństwa teleinformatycznego;
g) sterowniki PLC;
h) panele operatorskie HMI;
i) systemy SCADA;
j) pozostałe urządzenia i systemy przemysłowe objęte zakresem projektu.

2. Wymagania dotyczące inwentaryzacji

2.1. Wykonawca zobowiązany jest do identyfikacji i udokumentowania aktywów objętych zakresem usługi.

2.2. Dla każdego zidentyfikowanego aktywa należy określić, w zakresie możliwym do ustalenia, co najmniej:

a) unikalny identyfikator;
b) nazwę i typ urządzenia lub systemu;
c) producenta i model;
d) numer seryjny, jeżeli jest dostępny;
e) lokalizację;
f) funkcję i przeznaczenie;
g) adresację sieciową;
h) system operacyjny lub wersję oprogramowania układowego (firmware);
i) właściciela lub jednostkę odpowiedzialną;
j) poziom krytyczności;
k) istotne zależności komunikacyjne z innymi aktywami.

2.3. Inwentaryzacja musi umożliwiać rozróżnienie aktywów należących do infrastruktury IT i OT.

2.4. Wykonawca zobowiązany jest do identyfikacji podstawowych zależności pomiędzy systemami informatycznymi i przemysłowymi.

3. Sposób realizacji inwentaryzacji

3.1. Inwentaryzacja może być prowadzona z wykorzystaniem narzędzi programowych, danych z istniejących systemów, analizy konfiguracji oraz oględzin infrastruktury.

3.2. W przypadku infrastruktury OT/ICS/IIoT pozyskiwanie informacji musi odbywać się metodami niezakłócającymi pracy urządzeń i procesów technologicznych.

3.3. Aktywne skanowanie urządzeń przemysłowych dopuszcza się wyłącznie po uzgodnieniu z Zamawiającym oraz potwierdzeniu bezpieczeństwa danej metody.

3.4. Wykonawca zweryfikuje zgodność uzyskanych danych ze stanem faktycznym w zakresie uzgodnionym z Zamawiającym.

4. Dokumentacja inwentaryzacyjna

4.1. Wykonawca przekaże Zamawiającemu rejestr aktywów w formacie edytowalnym, umożliwiającym jego dalszą aktualizację.

4.2. Dokumentacja musi obejmować:

a) wykaz aktywów IT;
b) wykaz aktywów OT/ICS/IIoT;
c) schemat logiczny infrastruktury sieciowej;
d) schemat stref i połączeń IT–OT;

e) wykaz podstawowych zależności komunikacyjnych;
f) wykaz stwierdzonych braków lub niezgodności danych inwentaryzacyjnych.

4.3. Rejestr aktywów powinien umożliwiać jego późniejsze wykorzystanie w procesach zarządzania bezpieczeństwem informacji i aktualizacji ewidencji infrastruktury.

3.8. Oprogramowanie DLP – O26

1. Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, uruchomienie, systemu zapobiegania nieuprawnionemu ujawnieniu i wynoszeniu danych z komputerów końcowych. Ilość: 1 komplet obejmujący równoczesną ochronę co najmniej 15 komputerów z systemem Windows wspieranym przez dostawcę rozwiązania.Dopuszcza się samodzielne oprogramowanie Endpoint DLP, moduł platformy UEM albo współpracujące komponenty. Wymagania dotyczą wynikowego działania całości. System ma umożliwiać centralną administrację z infrastruktury Zamawiającego (on-premises); rozwiązanie korzystające z usług chmurowych dopuszcza się wyłącznie jako funkcje pomocnicze, o ile ochrona i zarządzanie pozostają dostępne w modelu wskazanym w ofercie, a transfer danych poza organizację jest jawny i uzgodniony.
2. Wymagania minimalne

2.1 Ochrona co najmniej 15 komputerów Windows jednocześnie; agent lub równoważny mechanizm wymuszający polityki na chronionym urządzeniu.

2.2 Centralna konsola pozwala tworzyć, przypisywać, zmieniać i wycofywać polityki dla urządzenia lub grupy urządzeń.

2.3 Wykrywanie informacji według co najmniej jednego konfigurowalnego kryterium odnoszącego się do zawartości danych, np. wzorca tekstowego, wyrażenia regularnego lub słów kluczowych; możliwe zastosowanie własnego kryterium administratora.

2.4 Przypisanie wykrytej informacji do kategorii chronionej oraz odmienne potraktowanie pliku neutralnego niespełniającego kryterium.

2.5 Tryb monitorowania (rejestracja bez blokady) oraz tryb egzekwowania (blokada operacji zgodnej z polityką), konfigurowalne dla wybranej grupy lub urządzenia.

2.6 Kontrola wynoszenia danych sklasyfikowanych jako chronione na wymienny nośnik pamięci USB; co najmniej blokada skopiowania danych chronionych przy możliwości skopiowania danych neutralnych zgodnie z polityką.

2.7 Kontrola co najmniej jednego dodatkowego kanału przesyłania danych: poczta, przeglądarka lub aplikacja chmurowa. Oferent wskaże nazwę wspieranej aplikacji i czynność podlegającą blokowaniu.

2.8 Możliwość ustanowienia i cofnięcia co najmniej jednego wyjątku dla zatwierdzonego przypadku (np. użytkownika, urządzenia lub aplikacji), z zachowaniem ochrony pozostałych przypadków.

2.9 Rejestracja zdarzeń zawierająca co najmniej czas, identyfikator komputera, typ kanału/operacji, zastosowaną politykę i rezultat; bez konieczności utrwalania pełnej zawartości chronionych plików.

2.10 Przeglądanie i eksport zestawienia zdarzeń z konsoli, co najmniej do CSV lub PDF.

2.11 Szyfrowanie połączenia do konsoli (HTTPS/TLS), uwierzytelnianie administratora oraz możliwość uwierzytelniania dwuskładnikowego lub integracji z usługą zewnętrzną zapewniającą drugi składnik.

2.12 Udokumentowana procedura wykonania i odtworzenia kopii zapasowej ustawień i polityk.

2.13 Prawo produkcyjnego użytkowania wszystkich wymaganych funkcji dla 20 komputerów przez co najmniej 36 miesięcy od odbioru, bez nieujawnionych opłat. Dopuszcza się licencje nieodpłatne, bezterminowe i komercyjne, bez ograniczenia do konkretnej edycji.

2.14 Jeśli produkt wykorzystuje wersję próbną z szerszym zakresem funkcji, wykonawca musi wykazać dostępność wszystkich funkcji obligatoryjnych na licencji docelowej (np. po zakończeniu okresu próbnego).

2.15 Wykonawca przekaże dokumentację powdrożeniową, spis objętych komputerów, eksport/ewidencję polityk, procedurę odtworzenia i instruktaż minimum jednego administratora.

3. Wdrożenie i zasady odpowiedzialności

- Wykonawca instaluje rozwiązanie, obejmuje ochroną 20 wskazanych komputerów, definiuje kryterium sztucznych danych testowych, politykę audytu, politykę blokowania, wyjątek i raport.
- Działania wdrożeniowe nie mogą zakłócić systemów OT/ICS. Testy przeprowadza się na stacjach testowych lub za zgodą Zamawiającego, na sztucznych danych, bez kopiowania informacji rzeczywistych.
- Wykonawca odpowiada za kompletność wszystkich oferowanych komponentów, interoperacyjność, aktualizacje bezpieczeństwa i wsparcie konfiguracji w okresie określonym umową.

3.9. UTM – S07 – 3 szt.

3.9.1. Nietechniczne cechy urządzeń

1) Przedmiot zamówienia musi być legalny, fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu, spełniający normy CE. Nie dopuszcza się urządzeń typu refurbished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
2) Projekt przewiduje 1 jednostkę IT oraz UTM Główny i UTM OŚ w OT.
3) Zamawiający wymaga, aby wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 4 miesięcy przed terminem składania ofert.
4) Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili, i co najmniej w okresie 4 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający

przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania

5) Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta.

3.9.2. Dodatkowe systemy zewnętrzne

Zamawiający dopuszcza, aby całościowy system bezpieczeństwa był zbudowany w oparciu o wymagane komponenty opisane w OPZ wraz z elementami dodatkowymi, których zastosowanie jest opcjonalne i dobrowolne. Decyzja o ich zastosowaniu leży w gestii Wykonawcy – jeżeli uzna on, iż dla osiągnięcia opisanych wymagań niezbędne są dodatkowe systemy zewnętrzne to Zamawiający zezwala na ich zastosowanie pod warunkami opisanymi poniżej:

1) stosowanie dodatkowych systemów nie może dotyczyć funkcji ochronnych NGFW (np. wykrywania aplikacji, obsługi IPS, AV czy NAT);
2) stosowanie dodatkowych systemów nie może powodować ominięcia reguł bezpieczeństwa

Przykładowo stosowanie dodatkowych systemów jest dopuszczalne, gdy są one konieczne np. dla:

1) weryfikacji tożsamości użytkowników – system uwierzytelniania;
3) realizacji funkcji zarządzania firewallem i uprawnieniami administratorów;
4) zatwierdzania zmian w konfiguracji;
5) realizacji funkcji inspekcji ruchu SSL;
6) realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania.

   Systemy wspomagające muszą być zaoferowane w pełnym wsparciem producenta co oznacza wymóg zaoferowania wszystkich pakietów serwisowych dostępnych dla danego rozwiązania,

   W przypadku stosowania systemów wspomagających Zamawiający wymaga by były one oferowane przez tego samego producenta co oferowany system firewall i całościowo serwisowane przez tego producenta.

   Zamawiający wymaga również, aby wszystkie dostarczane systemy wspomagające były sprawdzone w praktyce rynkowej i spełniały wymagania w tym obszarze analogicznie do firewalli, oznacza to, iż oprogramowanie systemowe realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 4 miesięcy przed terminem składania ofert.

   Zapewnienie redundancji nie jest wymagane dla usług realizowanych z chmury Threat Intelligence producenta oferowanego rozwiązania

1) Firewall musi być dostarczony w postaci dedykowanego rozwiązania sprzętowo-programowego – tzw. appliance.
2) Cechy wydajnościowe:

a. 1.5 Gbps przepustowości Firewall/kontroli aplikacji;

b. 0.8 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;
c. 0.5 Gbps dla IPsec VPN;
d. 64 000 jednoczesnych sesji;
e. 11 000 nowych połączeń na sekundę;
f. 25 stref bezpieczeństwa;
g. Lokalna przestrzeń pamięci co najmniej o pojemności 128GB przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi)

3) Cechy urządzenia – minimalna wymagana ilość interfejsów, zasilanie:

a. Wysokość maksymalnie 1U, urządzenie należy dostarczyć razem z zestawem montażowym w postaci półki do szafy RACK 19";
b. dwa redundantne zasilacze AC 230V z kompletami kabli;
c. 4 porty 1 GigabitEthernet RJ45
d. 4 porty 1 GigabitEthernet RJ45 z osbługą PoE
e. 1 port typu combo (SFP lub RJ45) 1 GigabitEthernet
f. 1 port konsolowy RJ45
g. 1 port konsolowy Micro USB
h. 2 porty USB
i. 1 dedykowany port zarządzający typu combo (SFP lub RJ45) 1 GigabitEthernet

3.9.3. Wymagania funkcjonalne dla rozwiązań NGFW:

UWAGA: Wszystkie wymienione poniżej funkcje muszą być dostępne i realizowane przez firewall jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenie lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego.
Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.

3.9.4. Cechy NGFW

1) Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 5000 aplikacji predefiniowanych przez Producenta.
2) Transparentne ustalenie tożsamości użytkowników
3) Możliwość rozbudowy o realizowanie funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:

a) Intrusion Prevention System (IPS),

b) Antywirus (AV),
c) Anty-Spyware / Anty-Malware ,
d) ochrona DNS,
e) sandbox lokalny lub chmurowy tego samego producenta

4) Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory
5) System musi zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji

3.9.5. Silniki detekcyjne i ochronne NGFW

1) Możliwość licencyjnej rozbudowy o następujące funkcjonalności związane z IPS, AV, Anty-Spyware:

a) Bazy sygnatur IPS, AV, Anty-Spyware (lub innego silnika, jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, regularnie aktualizowane w sposób automatyczny.
b) Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.
c) Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.
d) Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa. Nie dopuszcza się by IPS i AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego, gdzie administrator nie ma możliwości konfiguracji jaka część ruchu będzie podlegała inspekcji i w jakim zakresie.
e) Wykrywanie aktywności sieci typu Botnet.

2) Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.
3) Możliwość rozbudowy o funkcję filtrowania ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron.

a) Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp)
b) Ocena strony musi obejmować określenie ryzyka do niej przypisanego (co najmniej wysokie-średnie-niskie).
c) Musi być zapewniona możliwość tworzenia własnych list stron (whitelist oraz blacklist) bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta z możliwością konfiguracji, gdzie własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.

4) Możliwość rozbudowy o funkcję ochrony przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem

a) możliwość przesyłania do systemu sandbox (tego samego producenta co firewall) plików zdefiniowanych przez administratora (co najmniej exe, dll, java, MS Office, pdf). Zamawiający dopuszcza by odbywało się to poprzez dedykowany mechanizm wbudowany w urządzenie lub przez jeden z wymaganych silników detekcyjnych przy czym funkcja ta musi mieć możliwość wskazania/wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno kierunku transmisji (ruch wchodzący/wychodzący ze wskazanej strefy bezpieczeństwa), adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy

b) dopuszcza się zarówno realizację sandboxa w postaci chmury producenta jak i rozwiązania lokalnego. W tym drugim przypadku wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanym firewallem. W przypadku rozwiązania chmurowego analiza plików musi odbywać się na terenie Polski.

c) Bez względu na użyte rozwiązanie, wymaga się wydajności zapewniającej jednoczesną analizę minimum 20 plików/próbek w tzw. VM Sandboxing (rozumiana jako realizacja funkcjonalności sandbox polegająca na wykorzystaniu instancji maszyn wirtualnych z określonymi systemami operacyjnymi i zestawem zainstalowanych aplikacji do zdetonowania/uruchomienia, a następnie analizy podejrzanego pliku pod kątem jego potencjalnie negatywnego wpływu na komputery klienckie lub serwery).

d) Jednoczesna analiza 20 próbek/plików musi być zapewniona bez względu na to czy pliki te będą wysyłane automatycznie przez firewall czy manualnie przez administratora czy też będzie to mieszana grupa plików pochodząca zarówno bezpośrednio z firewalla, jak też od administratorów

5) Możliwość rozbudowy o ochronę DNS co najmniej w zakresie:

a) wykrywanie zapytań do domen złośliwych.

b) możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)

c) wykrywanie domen dynamicznych Dynamic DNS

6) Urządzenie musi umożliwiać uruchomienia funkcjonalności SD-WAN. Firewall musi weryfikować stan łącz w czasie rzeczywistym i w sposób dynamiczny wybierać optymalne łącze. Wymagane algorytmy wyboru łącza to: najlepsza dostępna, w kolejności od pierwszej do ostatniej, wagowa.

a) W zakresie SD-WAN urządzenie musi zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, zmienności opóźnienia, procentowej wartości traconych pakietów).

b) Monitoring parametrów SLA musi odbywać się nie tylko poprzez weryfikację drugiej strony tunelu IPSec VPN, ale także w oparciu o określony adres IP, FQDN

c) Urządzenie firewall musi posiadać osobny zestaw polityk definiujący reguły SD-WAN rozdzielny od polityk bezpieczeństwa.

d) Dla aplikacji wrażliwych na parametry jakościowe musi istnieć możliwość przesyłania zduplikowanych pakietów (packet duplication), naprawy utraconych pakietów poprzez dodanie bitów parzystości przez stronę nadającą (Forward Error Correction)

3.9.6. Deszyfracja ruchu

1) Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3).

3.9.7. Obsługa VPN oraz funkcji sieciowych

1) Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.
2) Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN.

a) Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW- obsługa co najmniej 1500 tuneli/użytkowników.
b) Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS.
c) Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewalla.
d) Jeżeli oprogramowanie klienta jest dodatkowo licencjonowane przez producenta wówczas należy przewidzieć je dla 2000 użytkowników/urządzeń oraz zapewnić możliwość licencyjnej rozbudowy do 3000.
e) oprogramowanie klienta musi mieć możliwość zdalnej kontroli, minimum sprawdzenie wersji oraz zdalną instalację aktualizacji.

3) Obsługa protokołów routingu: OSPFv2 i OSPFv3, BGP4;
4) Obsługa 4094 VLAN zgodnych z 802.1q.
5) Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.
6) Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
7) Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
8) Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
9) Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).

3.9.8. Uwierzytelnienie i ustalanie tożsamości użytkowników

1) Transparentne ustalenie tożsamości w oparciu o:

a) integrację z kontrolerem domeny Active Directory;

b) integrację z serwerami LDAP;
c) integrację z serwerami terminalowymi;
d) integrację bazującą na informacji z logów SYSLOG lub RADIUS pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX;
2) Firewall musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.
3) Uwierzytelnianie administratorów NGFW za pomocą:
a) bazy lokalnej;
b) zewnętrznej usługi katalogowej dostępnej po LDAPS;
c) RADIUS lub TACACS+.

3.9.9. Zarządzenie urządzeniami NGFW

4) Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez Interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora – bez konieczności korzystania z centralnych narzędzi zarządzania.
5) Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.
6) Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian (m.in. polityk, konfiguracji interfejsów, routingu itp.), ze wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

3.9.10. Interpretacja parametrów wydajnościowych NGFW

1) Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji - rozwiązanie pozwoli na:
a. wykrycie aplikacji,
b. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
2) Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji/IPS/ Antywirus /Antymalware - rozwiązanie pozwoli na:
a. wykrycie aplikacji,
b. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych,
c. inspekcje IPS całego ruchu,
d. inspekcję antywirusową całego ruchu,
e. inspekcję antymalware/AntySpyware całego ruchu,
f. przesyłanie plików do sandboxa lokalnego i/lub chmurowego,

g. przechwytywanie i blokowanie plików określonego typu.
h. logowanie zdarzeń

Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

3.9.11. ZAAWANSOWANA OCHRONA DNS

Zaawansowana ochrona DNS w trybie rzeczywistym. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko i wyłącznie w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej

I. wykrywanie zapytań do domen złośliwych.
II. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)
III. wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)
IV. wykrywanie domen fast flux
V. wykrywanie domen dynamicznych Dynamic DNS
VI. wykrywanie domen nowo rejestrowanych – Newly-registered-domain
VII. wykrywanie domen strategically-aged-domain
VIII. wykrywanie domen stockpiled
IX. wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych
X. wykrywanie ataków DNS Tunneling, w tym ultra-slow DNS Tunneling
XI. wykrywanie ataków na rekordy DNS, w tym CNAME cloaking, Wildcard DNS i Dangling DNS
XII. wykrywanie ataków na protokół DNS

3.9.12. OCHRONA Z WYKORZYSTANIEM MECHANIZMÓW MACHINE LEARNING–

Urządzenie NGFW musi pozwalać na blokowanie zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanego dynamicznie przez producenta. Wykrywanie i blokowanie złośliwych treści musi odbywać się lokalnie na urządzeniu, jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych oraz funkcji filtrowania URL. Funkcja wykrywania zagrożeń z wykorzystaniem mechanizmów ML musi być dostępna co najmniej dla:

I. złośliwych plików wykonywalnych (PE);
II. złośliwych skryptów PowerShell;
III. złośliwych skryptów JavaScript;
IV. ataków phishing;

Dodatkowo urządzenia firewall muszą umożliwiać wykorzystanie chmurowego mechanizmu analitycznego do analizowania ruchu pod kątem zaawansowanych zagrożeń C2 (command-and-control) i spyware w czasie rzeczywistym, aby chronić użytkowników przed zagrożeniami typu zero-day. Silniki powinny być aktualizowane, bez konieczności pobierania na urządzenie pakietów aktualizacji lub obsługi procesów dodatkowo obciążających firewall. Analiza w chmurze powinna obsługiwać co najmniej pięć silników analitycznych dla zagrożeń opartych na C2 przez HTTP, HTTP2, SSL, nieznany ruch UDP i nieznanych ruch TCP.

Wykonawca, który deklaruje spełnienie kryterium musi oferować urządzenia pozwalające blokowanie zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanego dynamicznie przez producenta. Wykrywanie i blokowanie złośliwych treści musi odbywać się lokalnie na urządzeniu, jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych oraz funkcji filtrowanie URL.

3.9.13. WYMAGANIA LICENCYJNE

1) Całość rozwiązania będzie pochodziła od jednego producenta i będzie objęta wsparciem serwisowym przez okres min. 36 miesięcy
2) W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 36 miesięcy.
3) Dla systemu firewall należy dostarczyć usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla następujących funkcji:
   a) Aktualizacje bazy aplikacji;
   b) realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN);
4) Dostarczone licencje i subskrypcje muszą zapewniać przez 36 miesięcy działanie wszystkich funkcji wymaganych jako obligatoryjne, w tym IPS, antymalware, filtrowania WWW/URL, ochrony DNS, sandboxingu oraz ochrony OT w określonym zakresie. Sama możliwość późniejszej rozbudowy licencyjnej nie stanowi spełnienia wymagania.

3.10. Testy bezpieczeństwa infrastruktury IT/OT/ICS/IIoT – U02

1. Przedmiot i zakres usługi
1.1. Przedmiotem zamówienia jest przeprowadzenie testów bezpieczeństwa infrastruktury

teleinformatycznej i przemysłowej Zamawiającego objętej projektem, w szczególności w zakresie identyfikacji podatności, błędów konfiguracyjnych oraz weryfikacji skuteczności zastosowanych zabezpieczeń.

1.2. Testy obejmują infrastrukturę IT/OT/ICS/IIoT, w zakresie uzgodnionym z Zamawiającym, w szczególności:

a) urządzenia i infrastrukturę sieciową;
b) serwery fizyczne i wirtualne oraz systemy operacyjne;
c) urządzenia UTM/NGFW oraz mechanizmy ochrony sieciowej;
d) segmentację sieci i komunikację pomiędzy strefami IT i OT;
e) mechanizmy uwierzytelniania i kontroli dostępu;
f) mechanizmy dostępu zdalnego, w tym VPN;
g) systemy i urządzenia OT/ICS/IIoT, w zakresie możliwym do bezpiecznego przeprowadzenia badań.

1.3. Celem usługi jest określenie poziomu bezpieczeństwa badanej infrastruktury, identyfikacja podatności i nieprawidłowości oraz przygotowanie rekomendacji działań naprawczych.

2. Skaner podatności

2.1. Wykonawca zapewni, w ramach ceny zamówienia, instalację i konfigurację aktywnego skanera podatności infrastruktury IT.

2.2. Dopuszcza się zastosowanie rozwiązania open source lub komercyjnego, pod warunkiem spełnienia wymaganych funkcjonalności.

2.3. Skaner musi umożliwiać co najmniej:

a) aktualizację bazy podatności;
b) wykonywanie skanowania uwierzytelnionego i nieuwierzytelnionego;
c) identyfikację znanych podatności bezpieczeństwa;
d) prezentację wyników skanowania;
e) sporządzanie raportów zawierających wykryte nieprawidłowości i podatności.

2.4. Skaner musi zostać przekazany Zamawiającemu wraz z dostępem administracyjnym oraz instrukcją eksploatacji.

2.5. Wykonawca zapewni uruchomienie skanera w środowisku wskazanym przez Zamawiającego oraz przeprowadzi weryfikację jego poprawnego działania.

3. Planowanie i realizacja testów bezpieczeństwa

3.1. Przed rozpoczęciem testów Wykonawca przedstawi Zamawiającemu do zatwierdzenia plan testów bezpieczeństwa.

3.2. Plan musi określać co najmniej:

a) wykaz zasobów i systemów objętych badaniem;
b) zakres i metody przeprowadzania testów;
c) harmonogram realizacji;
d) ograniczenia i wyłączenia dotyczące badanej infrastruktury;
e) zasady bezpieczeństwa prowadzenia testów;
f) warunki przerwania lub wstrzymania testów w przypadku stwierdzenia ryzyka zakłócenia pracy infrastruktury.

3.3. Wykonawca przeprowadzi testy obejmujące co najmniej:

a) identyfikację znanych podatności systemów i urządzeń;
b) analizę konfiguracji zabezpieczeń;
c) weryfikację segmentacji sieci;

d) analizę zasad dostępu do urządzeń i systemów;
e) weryfikację zabezpieczeń dostępu zdalnego;
f) ocenę potencjalnych zagrożeń wynikających z wykrytych nieprawidłowości.

3.4. Zakres i sposób prowadzenia testów muszą być dostosowane do charakteru infrastruktury Zamawiającego i uwzględniać wymagania ciągłości działania systemów IT oraz OT.

4. Testy bezpieczeństwa infrastruktury OT/ICS/IIoT

4.1. W środowisku OT/ICS/IIoT pierwszeństwo mają metody pasywne oraz analiza konfiguracji urządzeń i systemów.

4.2. Aktywne skanowanie urządzeń i systemów OT/ICS/IIoT wymaga uprzedniego zatwierdzenia przez Zamawiającego.

4.3. Przed przeprowadzeniem aktywnych testów infrastruktury OT Wykonawca zobowiązany jest uwzględnić zalecenia producentów urządzeń i systemów oraz uzgodnić z Zamawiającym odpowiednie okno serwisowe.

4.4. Zabrania się wykonywania nieuzgodnionych działań, które mogłyby spowodować zatrzymanie urządzeń, zmianę parametrów technologicznych, utratę dostępności lub zakłócenie funkcjonowania systemów sterowania i monitorowania procesów technologicznych.

4.5. W przypadku stwierdzenia ryzyka zakłócenia pracy infrastruktury Wykonawca zobowiązany jest do wstrzymania testów i uzgodnienia z Zamawiającym dalszego sposobu ich realizacji.

4.6. Jeżeli przeprowadzenie określonego testu nie jest możliwe bez ryzyka dla ciągłości działania infrastruktury, Wykonawca wskaże ograniczenie w raporcie oraz zastosuje możliwą do bezpiecznego wykonania metodę alternatywną.

5. Raport z testów bezpieczeństwa

5.1. Po zakończeniu testów Wykonawca opracuje i przekaże Zamawiającemu raport zawierający co najmniej:

a) wykaz przebadanych zasobów;
b) zastosowane metody testowania;
c) zakres przeprowadzonych badań;
d) wykaz wykrytych podatności i nieprawidłowości;
e) ocenę poziomu ryzyka;
f) opis potencjalnych skutków wykrytych podatności;
g) rekomendacje działań naprawczych;
h) wykaz testów niewykonanych wraz z uzasadnieniem;
i) ocenę ryzyk pozostających po zakończeniu prac.

5.2. Raport musi umożliwiać Zamawiającemu identyfikację zasobów wymagających działań naprawczych oraz określenie priorytetów usuwania stwierdzonych nieprawidłowości.

5.3. Wyniki testów zostaną przekazane w postaci elektronicznej, w formacie umożliwiającym ich przeglądanie i archiwizację.

6. Działania naprawcze i retesty

6.1. Wykonawca zobowiązany jest do usunięcia stwierdzonych niezgodności dotyczących rozwiązań dostarczonych lub skonfigurowanych przez niego w ramach niniejszego zamówienia.

6.2. Po usunięciu niezgodności Wykonawca przeprowadzi ponowne testy (retesty), których celem będzie potwierdzenie skuteczności zastosowanych działań naprawczych.

6.3. Wyniki retestów muszą zawierać co najmniej:

a) identyfikację weryfikowanej nieprawidłowości;
b) informację o wykonanym działaniu naprawczym;

c) wynik ponownej weryfikacji;
d) status usunięcia nieprawidłowości;
e) wskazanie ryzyk pozostających po przeprowadzeniu działań naprawczych.

6.4. W przypadku podatności dotyczących systemów lub urządzeń nieobjętych obowiązkiem naprawy przez Wykonawcę, Wykonawca przedstawi Zamawiającemu rekomendacje dotyczące sposobu ograniczenia ryzyka.

3.11. Urządzenie NAS – S21 – 1 szt.

Przedmiotem zamówienia jest dostawa 1 szt. Urządzenia przeznaczonej do bezpiecznego przechowywania i ochrony danych oraz realizacji funkcji zintegrowanego systemu wykonywania, zarządzania, weryfikacji i odtwarzania kopii zapasowych klasy Backup Appliance.

3.6.1 Zamawiający wymaga rozwiązania przeznaczonego do realizacji zadań związanych z cyberodpornym backupem, w szczególności zapewniającego mechanizmy ograniczające skutki awarii, utraty danych oraz incydentów typu ransomware.

3.6.2 Wymagane funkcjonalności urządzenia, w tym mechanizmy kopii niezmiennych Immutable/WORM, izolacji Air Gap, automatycznej weryfikacji kopii, natychmiastowego przywracania, deduplikacji oraz lokalnego uruchamiania środowisk z kopii zapasowych, stanowią element wymaganego poziomu odporności i odtwarzalności infrastruktury Zamawiającego.

3.6.3 Nie dopuszcza się zaoferowania urządzenia pełniącego wyłącznie funkcję przestrzeni dyskowej lub repozytorium danych, które nie zapewnia wymaganych funkcji tworzenia, zarządzania i odtwarzania kopii zapasowych.

4 Urządzenie musi spełniać co najmniej poniższe wymagania:

Urządzenie musi spełniać co najmniej poniższe wymagania:

1. Obudowa: Tower.

2. Procesor: minimum dwurdzeniowy procesor o taktowaniu bazowym 2,6 GHz, osiągający maksymalnie 3,1 GHz z wykorzystaniem technologii Turbo Boost.

3. Pamięć RAM: minimum 16 GB pamięci DDR4.

4. Dyski twarde i pamięć Cache:

4.1. Dyski HDD: urządzenie musi być fabrycznie wyposażone przez producenta w minimum 4 dyski twarde 3,5" z interfejsem SATA, o pojemności minimum 8 TB każdy.

4.2. Dyski NVMe: wraz z urządzeniem producent musi dostarczyć minimum 2 dyski M.2 NVMe klasy korporacyjnej, o pojemności minimum 400 GB każdy, przeznaczone do wykorzystania jako pamięć podręczna Cache.

4.3. Jednorodność rozwiązania: urządzenie główne oraz dyski HDD i NVMe muszą pochodzić od tego samego producenta i stanowić integralne elementy zestawu, identyfikowane indeksem producenta.

5. Porty sieciowe: urządzenie musi posiadać minimum:

5.1. Port zarządzający: 1 × 1GbE RJ45 przeznaczony do zarządzania poza pasmem.

5.2. Port transmisji danych: 1 × 10GbE RJ45 przeznaczony do przesyłania danych.

6. Wake on LAN/WAN: urządzenie musi obsługiwać funkcję Wake on LAN/WAN.
7. Obsługiwane poziomy RAID:
7.1. RAID 5: przeznaczony dla przestrzeni dyskowej wykorzystywanej do przechowywania kopii zapasowych.
7.2. RAID 1: przeznaczony dla pamięci podręcznej Cache.
8. Klaster zarządzający:
8.1. Skalowalność kontrolera klastra: obsługa minimum 30 serwerów oraz minimum 1 500 instancji roboczych w jednym klastrze.
8.2. Tryby pracy: możliwość pracy jako urządzenie samodzielne lub jako serwer zarządzany przez kontroler klastra.
8.3. Licencjonowanie klastra: w przypadku klastra składającego się z więcej niż 3 serwerów (nodów) dopuszcza się wymaganie dodatkowej licencji.
9. Wbudowany hipernadzorca:
9.1. Natychmiastowe przywracanie: możliwość jednoczesnego natychmiastowego przywrócenia minimum 2 maszyn wirtualnych.
10. Oprogramowanie systemowe: system operacyjny urządzenia musi być domyślnie inicjalizowany i skonfigurowany do realizacji funkcji wykonywania kopii zapasowych jako głównej i jedynej aplikacji dostępnej na oferowanym urządzeniu.
10.1. Automatyczna konfiguracja przestrzeni dyskowej: podczas procesu inicjalizacji urządzenia system musi automatycznie tworzyć przestrzeń dyskową opartą na RAID 5.
11. Centralne zarządzanie ochroną danych: dedykowany system musi zapewniać kompleksowe rozwiązanie do wykonywania kopii zapasowych w heterogenicznych środowiskach IT.
11.1. Zakres chronionych środowisk: rozwiązanie musi umożliwiać zdalne zarządzanie i monitorowanie ochrony co najmniej: komputerów, serwerów fizycznych, baz danych, maszyn wirtualnych oraz środowiska SaaS Microsoft 365.
11.2. Interfejs zarządzający: wszystkie funkcje ochrony muszą być dostępne z jednego centralnego interfejsu administracyjnego.
11.3. Deduplikacja: repozytorium kopii zapasowych musi obsługiwać deduplikację typu in-line.
12. Uwierzytelnianie połączeń agentowych: uwierzytelnianie sesji połączenia agentowego dla kopii obrazowych komputerów PC, Mac oraz serwerów fizycznych musi odbywać się za pomocą kluczy połączenia przypisanych do konkretnych planów ochrony.
12.1. Dane uwierzytelniające: nie dopuszcza się uwierzytelniania sesji agentowej za pomocą standardowych danych logowania w postaci loginu i hasła.
13. Kopie lokalne i zdalne: system musi umożliwiać wykonywanie kopii zapasowych zarówno lokalnie, jak i do lokalizacji zdalnej.
13.1. Harmonogramy: harmonogram wykonywania kopii lokalnych i zdalnych musi być konfigurowany niezależnie.
13.2. Plany ochrony: system musi umożliwiać tworzenie planów zawierających zbiorcze lub indywidualne ustawienia dla poszczególnych typów chronionych urządzeń.
14. Kopie niezmienne: rozwiązanie musi obsługiwać strukturę kopii niezmiennych (Immutable), opartą

na mechanizmie WORM (Write Once, Read Many).
14.1. Okres niezmienności: czas niezmienności określony w strukturze WORM musi być możliwy do skonfigurowania i realizowany niezależnie dla poszczególnych typów kopii zapasowych, w tym dla kopii lokalnych oraz zdalnych znajdujących się w ramach jednego planu ochrony.
15. Przywracanie danych: system musi obsługiwać co najmniej:
15.1. Przywracanie granularne: możliwość granularnego przywracania danych odpowiednio dla każdego obsługiwanego typu urządzenia.
15.2. Bare-metal recovery: możliwość odtworzenia typu bare-metal dla kopii komputerów PC oraz serwerów fizycznych.
15.3. Przywracanie pełne: możliwość pełnego przywracania maszyn wirtualnych oraz serwerów fizycznych.
15.4. Natychmiastowe przywracanie: możliwość natychmiastowego uruchomienia środowiska z kopii zapasowej.
15.5. P2V: możliwość przywrócenia serwera fizycznego jako maszyny wirtualnej, tj. Physical to Virtual (P2V).
16. Automatyczna weryfikacja kopii zapasowych: system musi umożliwiać weryfikację poprawności kopii zapasowej poprzez automatyczne rozpakowanie i uruchomienie obrazu backupu w ramach wbudowanego hipernadzorcy.
16.1. Rejestracja procesu weryfikacji: system musi umożliwiać utworzenie nagrania dokumentującego proces uruchomienia zweryfikowanej kopii zapasowej, z możliwością odtworzenia w trybie 3-krotnego przyspieszenia.
16.2. Pobieranie nagrania: nagranie musi być możliwe do pobrania bezpośrednio z graficznego interfejsu użytkownika systemu i odtworzenia na urządzeniu klienckim.
17. Izolacja sieciowa – Air Gap: system musi umożliwiać realizację izolacji sieciowej co najmniej poprzez:
17.1. Wyłączenie portu danych.
17.2. Wyłączenie urządzenia.
17.3. Izolację na poziomie zapory sieciowej: możliwość blokowania komunikacji z określonych adresów IP lub podsieci.
18. Gwarancja: wykonawca udzieli minimum 3-letniej gwarancji na całość oferowanego sprzętu.

3.12. Serwery fizyczne, w tym HA – S13 – 2 szt.

Wymagania	**Opis wymagań minimalnych**
Obudowa	Obudowa Rack o wysokości max 1U.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta i oznaczona jego znakiem

Wymagania	Opis wymagań minimalnych
	firmowym. Na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesory 16-rdzeniowy, klasy x86-64, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 50 000 pkt. w Average CPU Mark opublikowanym na stronie https://www.cpubenchmark.net/ dla konfiguracji jednoprocesorowej.
RAM	Zainstalowane min. 96 GB 5600MT/s
Dyski twarde	Zainstalowane 4 dyski SSD o pojemności co najmniej 1,9TB z możliwością konfiguracji RAID 10 Zainstalowane 4 dyski HDD o pojemności co najmniej 2,4TB z możliwością konfiguracji RAID 10
Kontroler dyskowy	Zainstalowany sprzętowy kontroler SAS 12Gb do obsługi dysków min 8 dysków wewnętrznych. Kontroler musi posiadać 4GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID - 0/1/10/5/6/
Interfejsy sieciowe/FC/SAS	Wbudowane min.: 1 interfejs sieciowy 1Gb full duplex Ethernet w standardzie BaseT; 2 interfejsy sieciowe 10Gb full duplex w standardzie SFP+, Porty muszą pozwalać na osiągnięcie maksymalnego transferu dla reprezentowanego standardu, interfejsy muszą być kompatybilne z flow control
Wbudowane porty	- z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny - z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwere Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.

Wymagania	Opis wymagań minimalnych
Video	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Zasilacze	Dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Zgodność z Systemami Operacyjnymi	Zgodność z systemami operacyjnymi Windows Server 2025, Ubuntu 22.04 LTS, 24.04 LTS, ESXI 8.0 Sterowniki do wszystkich podzespołów muszą być dostępne, dla każdej wymienionej platformy.
Bezpieczeństwo	Moduł TPM 2.0 Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS.
Karta Zarządzania	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, plyta glowna • Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.

Wymagania	Opis wymagań minimalnych
	• Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediow z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarzadzające umożliwiające:

Wymagania	Opis wymagań minimalnych
	- zarzadzenie infrastruktura serwerow,przelacznikow i storage bez udzialu dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwosc skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatow SSL tzw self-signed oraz zewnetrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zuzycia energii przez monitorowane urzędzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostepnosc konsoli monitorujacej na urzadzeniach przenosnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołaczanych systemow oraz szczegolowa inwentaryzacja - mozliwosc podnoszenia wersji oprogramowania dla komponentow zarzadzanych serwerow w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiazania - definiowanie polityk zgodnosci wersji firmware komponentow zarzadzanych urzadzen - definiowanie roli uzytkownikow oprogramowania - obsluga REST API oraz Windows PowerShell - obsluga SNMP, SYSLOG, Email Forwarding - autentykacja uzytkownikow: centralna (mozliwosc definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsluga single

Wymagania	Opis wymagań minimalnych
	sign on oraz SAML - obsluga tzw Forward Secrecy w komunikacji z zarzadzanymi urzadzeniami - przedstawianie historycznych aktywnosci uzytkownikow -blokowanie mozliwosci podlaczenia innego systemu zarzadzania do urzadzen zarzadzanych - tworzenie dziennika zdarzen ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Mozliwosc definiowania filtrow wyswietlanych zdarzen z dziennika. Mozliwosc eksportu dziennika zdarzen do pliku csv - Obsluga NTP - przesylanie alertow do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzetowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - mozliwosc automatycznego tworzenia zgloszen w centrum serwisowym producenta dla okreslonych zdarzen wraz z przesylem plikow diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
Oprogramowanie do zarządzania	Możliwość zainstalowania na dostarczonym serwerze oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Możliwość sprawdzenia stanu oraz konfiguracji macierzy RAID
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.

Wymagania	Opis wymagań minimalnych
	2) Serwer musi posiadać deklaracje CE. 3) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows] Windows Server 2022
Warunki gwarancji	1) Gwarancja producenta: **min. 24 miesiące lub dłużej zgodnie ze złożoną ofertą.** 2) Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7. 3) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 4) Naprawa ma się odbyć w siedzibie zamawiającego chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5) Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 7) Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 8) W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu wykonującego Serwis lub Producenta potwierdzające powyższe.

Wymagania	Opis wymagań minimalnych
	9) Firma serwisująca musi posiadać ISO9001 na świadczenie usług serwisowych oraz posiada autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty
Akcesoria	Wraz z każdym serwerem należy dostarczyć po: 2 kompatybilne wkładki SFP+ LC full duplex; dwa patchcordy LC o długości co najmniej 1,5 m.; przewody zasilające niezbędne do połączenia z dostarczonym UPS

3.13. System operacyjny i licencje dostępowe – O47

System Operacyjny	Zakup licencji Systemu Operacyjnego – Windows Server Standard 2025 zgodnie z licencyjnością procesorów i rdzeni dla urządzeń lub oprogramowanie równoważne. Opis równoważności dla Oprogramowania systemu operacyjnego: Zapewnienie p 1) Współpraca z procesorami o architekturze x86-64. 2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. 3) Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu. 4) Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2019. 5) Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 6) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

	8) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 9) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. 10) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 11) Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 12) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 13) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 14) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). 15) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, • Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. • PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: ○ Dystrybucję certyfikatów poprzez http, ○ Konsolidację CA dla wielu lasów domeny,

	○ Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen. • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). • Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersji 6 (IPv6). • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. 16) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 17) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 18) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 19) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania. Dodatkowo należy dostarczyć min. 10 licencje CAL dla urządzeń.

3.14. Profesjonalne wdrożenie i utrzymanie IT i OT – U09

3.14.1. Instalacja i wdrożenie rozwiązań z migracją – 1 szt.

1. Wymagania ogólne

1.1. Kompleksowa realizacja: Zamawiający wymaga zrealizowania kompleksowej dostawy, montażu i wdrożenia rozwiązania przy uwzględnieniu kompleksowego działania całości środowiska informatycznego.

1.2. Kierownik Projektu: Zamawiający wymaga wyznaczenia osoby w postaci Kierownika Projektu po

stronie Wykonawcy, jako pojedynczego punktu kontaktowego w zakresie:

- uzgodnienia harmonogramu prowadzonych prac,
- koordynowania i uzgadniania terminów dostaw,
- nadzorowania procesu i kompletności realizowania usług związanych z wdrożeniem,
- sporządzania protokołów dostaw i realizacji częściowej/całościowej zakresu wdrożenia.

1.3. Elementy dodatkowe: Zamawiający, w oparciu o własną wiedzę i doświadczenie, wyspecyfikował niezbędne elementy połączeniowe (wkładki, okablowanie), natomiast w przypadku gdy zajdzie taka potrzeba, wraz z dostarczoną Infrastrukturą Wykonawca zobowiązany jest dostarczyć niezbędne elementy, np. urządzenia i wyposażenie dotyczące redundancji łącz, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu jej do infrastruktury Zamawiającego.

2. Wdrożenie rozwiązań – prace montażowo-konfiguracyjne

2.1. Montaż urządzeń

- Zamontować w szafach RACK wszystkie dostarczone urządzenia (serwery, macierz, NAS, przełączniki itp.) oraz podzespoły (np. dyski, wkładki SFP).
- Zachować porządek i usunąć opakowania oraz zbędne pozostałości po procesie instalacji.

2.2. Okablowanie i patch panele

- Zamontować patch panel w szafie teleinformatycznej, zarobić i opisać gniazda według dostarczonego schematu.
- Podłączyć wszystkie przewody sieciowe w szafie rackowej (miedziane kat. 6 UTP lub światłowodowe), zapewnić potrzebne kable zasilające i listwy.
- Zrealizować połączenia z zachowaniem redundancji (co najmniej N+1) i agregacji łączy w oparciu o maksymalną przepustowość, np. SFP+ 10 Gbps.

2.3. Aktualizacja i konfiguracja urządzeń

- Zaktualizować firmware do najnowszej stabilnej wersji zalecanej przez producenta.
- Skonfigurować urządzenia w warstwie fizycznej i logicznej tak, aby były gotowe do pracy zgodnie z ustaleniami z Zamawiającym.
- Zainstalować i skonfigurować systemy operacyjne oraz niezbędne oprogramowanie na serwerach.
- Uruchomić macierz dyskową i skonfigurować dyski, np. w RAID 10.
- Przygotować serwer NAS do archiwizacji przyrostowej stacji roboczych i przedstawić administratorowi zasady obsługi.

2.4. Oznaczenia, testy i dokumentacja

- Opisać wszystkie porty w sposób trwały i widoczny w szafie rackowej.
- Przeprowadzić testy poprawności działania, w tym szybkości łączy, komunikacji, dostępu do zasobów i redundancji.
- Utworzyć dokumentację końcową obejmującą parametry, hasła i schematy oraz przekazać ją Zamawiającemu.

2.5. Zakres obowiązków Wykonawcy

- Zainstalować kompletne rozwiązanie, w tym sprzęt i okablowanie, w pomieszczeniu

serwerowni.

- Włączyć nowe urządzenia do infrastruktury Zamawiającego.
- Zapewnić, że wszystkie elementy (serwery, macierz, NAS, przełączniki, patch panele) są skonfigurowane i gotowe do użytkowania.
- Zrealizować montaż i konfigurację w terminach ustalonych z Zamawiającym, nawet w dni wolne od pracy Urzędu, o ile tak przewiduje umowa.

2.6. Termin wykonania prac instalacyjno-wdrożeniowych i oddanie systemu do eksploatacji

Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane w oparciu o współpracę z przedstawicielem Zamawiającego. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.

Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo-instalacyjnych, w godzinach od 8:00 do 15:30.

W tym czasie przedstawiciel Wykonawcy:

- zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji,
- dokona prezentacji działania systemu dla osoby wyznaczonej przez Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:
  - zastosowanej technologii serwerów,
  - zastosowanej technologii pamięci masowej,
  - wirtualizacji,
  - systemu backupu.

3. Wdrożenie i konfiguracja rozwiązań oraz hardening

3.1. UTM

3.1.1. Przygotowanie i aktualizacja urządzenia

- Zaktualizować oprogramowanie układowe (firmware) urządzenia UTM/firewall do najnowszej stabilnej wersji.
- Zarejestrować lub aktywować urządzenie na stronie producenta, jeśli jest to wymagane.
- Włączyć (aktywować) licencje oraz moduły funkcjonalne: AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email.

3.1.2. Integracja z infrastrukturą sieci

- Opracować projekt włączenia urządzenia do sieci LAN (lokalizacja, podsieci, VLAN).
- Skonfigurować podstawowe parametry sieciowe firewall (adresy interfejsów, DNS, NTP).
- Dopasować mechanizmy translacji adresów NAT do architektury sieci, np. przekierowania portów.
- Zastosować separację ruchu za pomocą VLAN, w tym VLAN dla serwerów, macierzy, stacji roboczych, gości itp.

3.1.3. Polityki dostępu i bezpieczeństwa

- Zbudować reguły bezpieczeństwa (Security Policies), minimalizujące dostęp na zasadzie

„allow-list” – pozwalać wyłącznie na określony ruch.

- Dostosować reguły do konkretnych VLAN i podsieci, w tym ruch pomiędzy serwerami i stacjami roboczymi.
- Zarządzać bramą (firewall) przez dedykowaną, zaufaną stację administracyjną lub segment sieci, ograniczając dostęp z innych lokalizacji.
- Testować działanie bramy, weryfikując, czy reguły blokują/pozwalają na ruch zgodnie z założeniami.

3.1.4. Rozszerzone moduły i inspekcja ruchu

IPS (Intrusion Prevention System):

- włączyć ochronę wybranych VLAN,
- zdefiniować reguły wykrywania i reagowania (block/alert),
- przetestować poprawność działania IPS na przykładowych próbach ataku.

Moduły antywirusowe, antyspyware, antyspam, blokowanie plików i filtrowanie URL:

- skonfigurować inspekcję protokołów HTTP, HTTPS, SMTP, FTP, POP3, IMAP,
- dodać reguły filtrowania treści, w tym kategorie stron WWW i niepożądane załączniki pocztowe,
- rozważyć integrację z kontrolą tożsamości, np. domeną AD lub innym rozwiązaniem.
- Włączyć funkcje DLP (Data Loss Prevention) lub Data Patterns, jeśli urządzenie i licencja je obsługuje, aby zapobiec wyciekom danych poufnych.
- Skonfigurować inspekcję SSL, jeśli urządzenie i polityka bezpieczeństwa na to pozwalają, aby analizować zaszyfrowany ruch pod kątem zagrożeń.

Dla obszaru OT Wykonawca uruchomi mechanizmy IPS z obsługą protokołów przemysłowych występujących w chronionych segmentach, wraz z niezbędnymi licencjami i aktualizacjami. Polityki muszą uwzględniać specyfikę urządzeń oraz ciągłość procesu technologicznego. Włączenie blokowania ruchu OT wymaga zatwierdzenia przez Zamawiającego; dopuszcza się początkowe uruchomienie w trybie detekcji i alarmowania. Wykonawca udokumentuje zakres ochrony, wyjątki i wyniki bezpiecznych testów.

3.1.5. Zdalny dostęp i VPN

- Skonfigurować SSL VPN dla pracowników zdalnych, gwarantując szyfrowanie połączeń i uwierzytelnienie użytkowników.
- Zastosować moduł uwierzytelnienia, np. konta domenowe, 2FA, do kontroli dostępu VPN.

3.1.6. Uwierzytelnianie i polityki użytkowników

- Zintegrować UTM z modułem uwierzytelnienia w oparciu o usługę domenową, np. Active Directory, lub dedykowany serwer RADIUS/TACACS+.
- Wykorzystać polityki dostępu oparte na użytkownikach (tożsamości), a nie tylko na IP/MAC.

3.1.7. Kontrola aplikacji i QoS

- Skonfigurować kontrolę aplikacji (App Control), ograniczając lub blokując niepożądane usługi, np. P2P, streaming w godzinach pracy.

3.1.8. Testowanie, audyt i raportowanie

- Skonfigurować logowanie i raportowanie (syslog, SNMP, integracja z SIEM), aby gromadzić i

analizować zdarzenia sieciowe.

3.1.9. Kopie zapasowe i utrzymanie

- Tworzyć regularne kopie zapasowe konfiguracji urządzenia i przechowywać je w bezpiecznym miejscu.
- Monitorować stabilność działania i reagować na wszelkie alerty, błędy lub anomalie w funkcjonowaniu urządzenia na wezwanie Zamawiającego.

3.2. Switching

3.2.1. Przygotowanie i audyt

- Przeprowadzić audyt obecnej infrastruktury – inwentaryzacja przełączników, portów, istniejących VLAN i adresacji.
- Zaktualizować firmware przełączników do najnowszej stabilnej wersji.
- Sprawdzić wymagania Zamawiającego w zakresie liczby VLAN, stref bezpieczeństwa i przepustowości łączy.

3.2.2. Topologia i połączenia fizyczne

- Zachować nadmiarowość połączeń (linków) i wdrożyć STP, np. RSTP lub MSTP, w celu zapobiegania pętlom.

3.2.3. Logiczna segmentacja – VLAN i routing

- Skonfigurować VLAN zgodnie z wydzielonymi strefami wskazanymi przez Zamawiającego.
- Rozplanować adresację IP (readresacja, jeśli potrzebna), tak aby poszczególne strefy VLAN miały własne podsieci.
- Skonfigurować trunking VLAN na portach łączących przełączniki CORE i IDF, aby propagować wszystkie potrzebne sieci VLAN.
- Upewnić się, że routing między VLAN-ami odbywa się przez UTM, aby egzekwować centralne polityki bezpieczeństwa.

3.2.4. Mechanizmy bezpieczeństwa warstwy 2

- Włączyć DHCP Snooping na interfejsach VLAN, aby zapobiegać atakom typu DHCP Starvation i rogue DHCP.
- Skonfigurować Dynamic ARP Inspection (DAI), weryfikując pary MAC-IP z bazą DHCP Snooping.
- Uaktywnić Port Security na portach przełączników, szczególnie w strefach końcówek biurowych, aby ograniczyć liczbę dozwolonych adresów MAC.
- Wdrożyć 802.1X (Network Access Control) na wskazanych portach dla uwierzytelniania i autoryzacji urządzeń/komputerów użytkowników, z użyciem certyfikatów lub kont domenowych, poprzez RADIUS lub alternatywną usługę.
- Rozważyć isolate-port lub Private VLAN, gdzie potrzebna jest dodatkowa izolacja, np. strefa gościnna.

3.2.5. STP i ochrona przed pętlami

- Uruchomić protokół drzewa rozpinającego STP/RSTP/MSTP na przełącznikach, zachowując spójność konfiguracji.
- Skonfigurować funkcje typu BPDU Guard, aby porty dostępu reagowały na nieautoryzowane

ramki BPDU.

- Wyłączyć lub ograniczyć zbędne protokoły, np. CDP, LLDP – w zależności od polityki – aby nie ujawniać niepotrzebnych informacji w sieci.

3.2.6. Dodatkowe zabezpieczenia i optymalizacje

- Włączyć Storm Control na interfejsach w celu przeciwdziałania atakom broadcast/multicast/unicast flood.
- Wyłączyć nieużywane porty fizyczne, a tam gdzie możliwe włączyć je w stan administracyjnie „down".

3.2.7. Integracja z systemami logowania i monitoringu

- Skonfigurować serwery NTP, np. firewall w klastrze, jako źródło czasu dla przełączników.
- Zainstalować serwer logów (open-source lub komercyjny) i skonfigurować przełączniki do wysyłania logów (syslog, SNMP traps) w trybie centralnym.
- Uruchomić system monitorowania z interfejsem graficznym, aby śledzić stan urządzeń (przełączniki, drukarki, UTM) i reagować na alerty. Monitoring obejmie infrastrukturę IT i OT objętą projektem, w tym serwery, usługi wirtualizacyjne, zasoby dyskowe, backup, urządzenia sieciowe, UTM, UPS oraz dostępne interfejsy diagnostyczne systemów OT. Wykonawca skonfiguruje pomiar dostępności, wykorzystania zasobów i stanu usług, progi alarmowe, powiadomienia oraz dashboardy. Dokumentacja wskaże monitorowane zasoby, zastosowane metody i ograniczenia monitorowania OT. Odbiór obejmie kontrolowany test niedostępności zasobu i przekroczenia progu alarmowego.
- Wykorzystać port SPAN (Switched Port Analyzer) lub RSPAN do przekazywania ruchu do IDS/IPS/SIEM, jeśli takie rozwiązania są w użyciu.

3.2.8. Testowanie i odbiór

- Sporządzić dokumentację powdrożeniową zawierającą schemat topologii, listę VLAN, reguły bezpieczeństwa oraz konfigurację protokołów.

3.2.9. Wykonawca przeprowadzi inwentaryzację aktywów IT/OT/ICS/IIoT objętych projektem, obejmującą urządzenia sieciowe, serwery, stacje robocze, systemy bezpieczeństwa oraz urządzenia i systemy przemysłowe, w szczególności PLC, HMI i SCADA. Rejestr będzie zawierał co najmniej identyfikator aktywa, typ, producenta i model, lokalizację, rolę, adresację, wersję systemu lub firmware, właściciela, krytyczność oraz istotne zależności komunikacyjne. Wykonawca przekaże rejestr w formacie edytowalnym oraz schemat stref i połączeń IT–OT. Pozyskiwanie informacji o OT musi odbywać się metodami niezakłócającymi procesu technologicznego.

3.3. System backupu

System musi zostać podłączony do klastra wirtualizacyjnego celem wykonywania backupu przyrostowego i pełnego maszyn wirtualnych, przechowywanych na serwerze backupu.

Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej.

3.3.1. Instalacja i licencjonowanie

- Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze.

- Aktywacja oraz instalacja niezbędnych licencji.
- Konfiguracja stacji zarządzającej.
- Dołączenie systemów zwirtualizowanych do systemu backupu.

3.3.2. Zadania backupu

Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:

- kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące,
- kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy,
- kopie wirtualnych maszyn muszą być wykonywane automatycznie według zadanego harmonogramu,
- musi istnieć możliwość odtworzenia:
  - całej wirtualnej maszyny,
  - dysku wirtualnej maszyny,
  - pojedynczych plików wirtualnej maszyny poprzez zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa.
- „Wykonawca skonfiguruje polityki backupu dla wszystkich systemów objętych zakresem, z harmonogramem, retencją, powiadomieniami, szyfrowaniem oraz testem odtworzeniowym. Odbiór nastąpi po wykonaniu i udokumentowaniu co najmniej: odtworzenia 1 pełnej maszyny wirtualnej, 1 pliku oraz 1 testu przywrócenia konfiguracji systemowej.”

3.3.3. Powiadomienia

Zdefiniowanie powiadomień o przebiegu zadania. Zamawiający wymaga skonfigurowania powiadomień na wskazany adres e-mail, zawierających co najmniej:

- nazwę zadania backupu,
- status zakończenia zadania backupu w przypadku niepowodzenia.

3.3.4. RPO i RTO

Na etapie wdrożenia należy ustalić z Zamawiającym:

- RPO – maksymalny dopuszczalny okres utraty danych, wyrażony czasem pomiędzy ostatnim odtwarzalnym punktem a wystąpieniem awarii.
- RTO – docelowy maksymalny czas przywrócenia wymaganej dostępności usługi po awarii..

3.4. Migracja danych

Migracja dotyczy przeniesienia obecnie użytkowanych i rozwijanych systemów informatycznych na nowe środowisko sprzętowe z wykorzystaniem wirtualizacji zasobów.

Systemy dziedzinowe muszą zostać przeniesione na nowe zasoby serwerowe oraz macierzowe.

Wykonawca odpowiada za przygotowanie środowiska docelowego, maszyn wirtualnych, systemów operacyjnych, zasobów dyskowych, połączeń i mechanizmów backupu. Migrację aplikacji dziedzinowych i ich baz danych wykonuje Zamawiający lub wskazani przez niego dostawcy. Wykonawca zapewni współpracę techniczną i diagnostykę środowiska docelowego. Odbiór prac

Wykonawcy obejmie sprawdzenie gotowości środowiska do uruchomienia migrowanych systemów. Do zadań Wykonawcy należy przygotowanie zaktualizowanych systemów operacyjnych zgodnie z wymaganiami Zamawiającego dotyczącymi konfiguracji maszyn wirtualnych.

Migracja danych musi uwzględniać współdzielenie zasobów oraz weryfikację ich poprawności i jakości technicznej, w szczególności w zakresie kompletności danych i rejestrów systemów dziedzinowych.

3.5. Instalacja i konfiguracja oprogramowania

3.5.1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT, z zachowaniem zgodności z ilością dostarczonych licencji.

3.5.2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu.

3.5.3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych i licencji. Wszelkie procedury rejestracyjne powinny zostać wykonane na danych dostarczonych przez Zamawiającego.

3.5.4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych.

3.5.5. Platforma kontenerowa. Wykonawca uruchomi platformę kontenerową dla komponentów cyberbezpieczeństwa wymagających takiego środowiska. Zakres obejmie konfigurację sieci i trwałych danych, kontrolę dostępu, zarządzanie obrazami i aktualizacjami, rejestrowanie zdarzeń, kopie zapasowe oraz odtwarzanie. Dokumentacja wskaże uruchomione komponenty i procedury ich utrzymania.

3.5.6. Wysoka dostępność. Wykonawca skonfiguruje środowisko wirtualizacyjne wykorzystujące dwa dostarczone serwery, z mechanizmem przełączenia usług po awarii hosta. Dokumentacja określi sposób działania pamięci masowej, zależności i pojedyncze punkty awarii. Dla wymaganej w projekcie dostępności NAS Wykonawca określi i wdroży mechanizm zapewniający ten rezultat; RAID nie będzie traktowany jako równoważny HA urządzenia.

3.6. Active Directory

3.6.1. Kontrolery domeny i usługi bazowe

- Wdrożyć główny kontroler domeny i kontroler zapasowy w celu zapewnienia wysokiej dostępności.
- Utworzyć struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.

3.6.2. Serwer plików i polityki uprawnień

Skonfigurować serwer plików (File Server) z właściwymi politykami uprawnień, tak aby były spełnione poniższe założenia:

- serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów,
- serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu,
- na serwerach plików muszą być skonfigurowane przydziały dyskowe dla użytkowników i grup; Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych

folderów,

- Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików; funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego,
- Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:
    - określenie daty, czasu i nazwy użytkownika, który usunął lub próbował usunąć plik/folder,
    - określenie daty, czasu i nazwy użytkownika, który zapisał lub próbował zapisać plik/folder,
    - określenie daty, czasu i nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień,
- zarządzać ustawieniami systemu za pomocą obiektów zasad grupy (GPO).

3.6.3. Hardening i bezpieczeństwo systemu

- Zaimplementować bazowe konfiguracje bezpieczeństwa, np. według zaleceń CIS.
- Włączyć inspekcję zdarzeń i skonfigurować centralne przechowywanie logów.
- Zabezpieczyć i skonfigurować zdalną administrację (RDP, PowerShell Remoting) z minimalizacją uprawnień,
- Ustawić narzędzia Microsoft Defender, w tym zaporę systemową, Application Guard oraz elementy Windows Defender Security Center.
- Ustawić woluminy dyskowe wirtualnych systemów, komputerów i laptopów (BitLocker).
- Chronić i konfigurować usługi DNS oraz DHCP zgodnie z wytycznymi bezpieczeństwa.

3.6.4. Zarządzanie certyfikatami

- Zainstalować i skonfigurować urząd certyfikacji (Certification Authority).
- Zaplanować i uruchomić wewnętrzną strukturę CA.
- Skonfigurować szablony certyfikatów.
- Wydać certyfikaty dla serwerów oraz stacji roboczych.
- Zastosować mechanizmy bezpieczeństwa poprzez możliwość backupu/archiwizacji kluczy prywatnych wydawanych certyfikatów.
- Zapewnić bezpieczną transmisję danych, na przykład poprzez wdrożenie SSL/TLS w usługach IIS.

3.6.5. Serwery uwierzytelniające

- Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych.
- Zamawiający wymaga uruchomienia co najmniej jednej instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.
- Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę.

- Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających, bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.

3.6.6. Zabezpieczanie dostępu zdalnego

- Wdrożyć bezpieczne połączenia RDP (TS Gateway) wraz z odpowiednimi regułami zapory systemowej.

3.6.7. Aktualizacje

Skonfigurować serwer WSUS umożliwiający instalację i centralne zarządzanie aktualizacjami stacji roboczych Windows według założeń:

- aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet,
- administrator zatwierdza aktualizacje do instalacji,
- stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu,
- Zamawiający wymaga skonfigurowania co najmniej:
    - systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje,
    - kategorii aktualizacji,
    - grup komputerów: KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST,
    - polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów,
    - zasad automatycznego zatwierdzania nowych aktualizacji.

3.6.8. Zarządzanie uprawnieniami i tożsamością

- Stosować mechanizmy Just Enough Administration (JEA).
- Włączyć kontrolę aplikacji (Windows Defender Application Control, WDAC) i skonfigurować ustawienia UAC dla użytkowników.

3.6.9. Bezpieczeństwo stacji roboczych

- Wdrożyć funkcję zabezpieczonego rdzenia (Secured-core PC) w systemach Windows 11 oraz izolację sprzętową (Core Isolation).
- Zarządzać najmniejszymi uprawnieniami (LPM) i kontrolować aplikacje (AppLocker lub WDAC) na stacjach użytkowników.
- Wdrożyć Software Restriction Policy.

3.6.10. Uruchomienie i skonfigurowanie serwera plików

Zamawiający wymaga uruchomienia oraz skonfigurowania serwerów plików tak, aby były spełnione poniższe założenia:

- serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów,
- serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu,
- na serwerach plików muszą być skonfigurowane przydziały dyskowe dla użytkowników i grup;

Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów,

- Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty" oraz „Pulpit" ze stacji roboczych na serwery plików; funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego,
- Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:
    - określenie daty, czasu i nazwy użytkownika, który usunął lub próbował usunąć plik/folder,
    - określenie daty, czasu i nazwy użytkownika, który zapisał lub próbował zapisać plik/folder,
    - określenie daty, czasu i nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.

3.7. Systemy operacyjne na bazie Linux

3.7.1. Kompleksowy opis zadań zabezpieczających serwer Linux

- Wyłączyć protokół IPv6, jeśli nie jest wykorzystywany.
- Włączyć audyt logów i monitorować zdarzenia w systemie.

3.7.2. Zabezpieczenie dostępu

- Skonfigurować serwer SSH w taki sposób, aby wyłączyć logowanie użytkownika root i korzystać z autoryzacji kluczami.
- Uruchomić narzędzie typu fail2ban lub podobne, aby blokować nieudane próby logowania.
- Włączyć blokowanie konta po określonej liczbie błędnych prób.

3.7.3. Segmentacja i ograniczanie usług

- Przeanalizować otwarte porty i wyłączyć wszystkie nieużywane.
- Usunąć zbędne aplikacje i wyłączyć niepotrzebne usługi działające w tle.

3.7.4. Zarządzanie uprawnieniami i polityki bezpieczeństwa

- Włączyć i skonfigurować SELinux lub AppArmor w celu ograniczenia dostępu aplikacji do zasobów systemowych.
- Korzystać z list ACL (Access Control Lists), aby precyzyjnie nadawać prawa do plików i katalogów.
- Zweryfikować konfigurację sudo i ograniczyć przywileje do niezbędnego minimum.

3.7.5. Zalecenia branżowe i compliance

- Porównać konfigurację systemu z wytycznymi branżowymi, np. CIS Benchmarks.

3.7.6. Fizyczne i sprzętowe środki bezpieczeństwa

- Wyłączyć obsługę zewnętrznych nośników USB, jeśli nie są niezbędne.
- Zainstalować oprogramowanie antywirusowe, uwzględniając polityki firmy i wymagania.

3.7.7. Usługi towarzyszące

- Skonfigurować serwer NTP, aby zapewnić spójność czasową w logach i procesach bezpieczeństwa.

3.8. System uwierzytelniania wieloskładnikowego (MFA)

3.8.1. Zintegrować system MFA i skonfigurować UTM do uwierzytelniania VPN za pomocą serwera RADIUS; zintegrować serwer z Active Directory poprzez LDAP. Wykonawca zainstaluje lub rozbuduje i skonfiguruje usługę RADIUS dla VPN oraz uwierzytelniania 802.1X w sieci przewodowej i bezprzewodowej. Zapewni integrację z Active Directory, konfigurację wymaganych certyfikatów i polityk, logowanie zdarzeń oraz test dopuszczenia i odmowy dostępu.
3.8.2. Skonfigurować uwierzytelnianie VPN z Active Directory z wymogiem systemu MFA poprzez LDAP.
3.8.3. Skonfigurować wymuszenie MFA przy logowaniu do Windows za pomocą kluczy YubiKey, zarządzane z poziomu centralnej konsoli.
3.8.4. Zainstalować agenta MFA poprzez GPO na komputerach użytkowników.
3.8.5. Zarejestrować klucze bezpieczeństwa dla 15 użytkowników.
3.8.6. Skonfigurować politykę logowania dla odpowiednich użytkowników w konsoli systemu MFA.
3.8.7. Wykonawca wdroży lub rozbuduje infrastrukturę PKI niezbędną do realizacji zabezpieczeń projektu, w tym uwierzytelniania i dostępu administracyjnego w obszarze IT/OT. Zakres obejmie konfigurację urzędu certyfikacji, szablonów i uprawnień, wydawanie, odnawianie i unieważnianie certyfikatów, udostępnianie informacji o ich statusie oraz kopie zapasowe i procedurę odtworzenia.
3.9. Wdrożenie dedykowanej stacji administracyjnej PAW – Privileged Access Workstation
W ramach usługi Wykonawca przygotuje dedykowaną stację roboczą z aktualnym systemem Windows, skonfigurowaną zgodnie z zasadami bezpiecznego dostępu uprzywilejowanego.
Na stacji zostaną zastosowane co najmniej następujące mechanizmy bezpieczeństwa:

- szyfrowanie dysku BitLocker z wykorzystaniem TPM,
- włączenie mechanizmów Secure Boot, TPM oraz zabezpieczeń opartych o wirtualizację,
- włączenie Credential Guard w celu ograniczenia możliwości kradzieży danych uwierzytelniających,
- konfiguracja Microsoft Defender Antivirus i zapory Windows Defender Firewall,
- zastosowanie polityk GPO ograniczających możliwość zmiany konfiguracji stacji przez użytkownika,
- ograniczenie uruchamiania nieautoryzowanego oprogramowania przy użyciu mechanizmów kontroli aplikacji, np. AppLocker lub Windows Defender Application Control,
- ograniczenie lub kontrola wykorzystania przenośnych nośników USB,
- automatyczne blokowanie stacji po określonym czasie bezczynności,
- instalowanie wyłącznie zatwierdzonych aktualizacji systemu i oprogramowania,
- przekazywanie istotnych logów bezpieczeństwa stacji do systemu SIEM/Wazuh.

Na PAW zostaną zainstalowane wyłącznie narzędzia niezbędne do administrowania infrastrukturą, w szczególności – zależnie od środowiska Zamawiającego:

- RSAT / Active Directory Users and Computers,
- Group Policy Management,
- DNS/DHCP Management,
- narzędzia AD CS/CA,
- PowerShell i Windows Terminal,

- Hyper-V Manager,
- Remote Desktop Client,
- klient SSH,
- konsole administracyjne systemów backupu, wirtualizacji i bezpieczeństwa,
- przeglądarka internetowa skonfigurowana wyłącznie do dostępu do zatwierdzonych lokalnych interfejsów administracyjnych, np. UTM, przełączników, macierzy, NAS, UPS, SIEM lub systemów OT.

3.9.2. Separacja od zwykłego stanowiska pracy

Na stacji PAW nie będą wykonywane czynności niezwiązane z administracją.

W szczególności stacja nie będzie wykorzystywana do:

- obsługi poczty elektronicznej,
- korzystania z komunikatorów,
- pracy z pakietem biurowym,
- pobierania przypadkowych plików z Internetu,
- korzystania z mediów społecznościowych,
- zwykłego przeglądania stron internetowych,
- wykonywania codziennej pracy użytkownika.

Administrator będzie posiadał oddzielne konto standardowe do codziennej pracy oraz dedykowane konto administracyjne wykorzystywane wyłącznie na PAW.

3.9.3. Dostęp do infrastruktury

PAW zostanie umieszczony w wydzielonym VLAN-ie administracyjnym / Management VLAN. Reguły firewall i ACL zostaną skonfigurowane w taki sposób, aby stacja mogła komunikować się wyłącznie z systemami, którymi administrator ma zarządzać.

Dostęp administracyjny do krytycznych systemów powinien być możliwy wyłącznie z PAW lub innych jednoznacznie wskazanych, zaufanych stanowisk administracyjnych.

W szczególności ograniczony zostanie dostęp administracyjny z typowych stacji użytkowników do Active Directory, kontrolerów domeny, CA, serwerów, hypervisorów, systemów backupu, UTM, przełączników, urządzeń sieciowych, NAS, SIEM oraz innych systemów infrastrukturalnych.

Dla kont uprzywilejowanych zostanie wdrożone silne uwierzytelnianie. W przypadku wykorzystania infrastruktury PKI Zamawiającego dostęp administratora może być zabezpieczony za pomocą YubiKey w trybie PIV wraz z certyfikatem wydanym przez AD CS/CA i kodem PIN.

3.9.4. Powiązanie z PAM/JIT

Stacja PAW będzie stanowiła zaufany punkt dostępu do mechanizmu zarządzania uprawnieniami uprzywilejowanymi PAM/JIT.

Docelowy model dostępu:

administrator → PAW → YubiKey/PIV → konto administracyjne → czasowe uprawnienie JIT → zarządzany system

Uprawnienia wysokiego poziomu, np. członkostwo w grupach administracyjnych, mogą być przyznawane wyłącznie na czas wykonywania określonego zadania i automatycznie wygasać po określonym czasie.

3.10. Wdrożenie systemu zarządzania dostępem uprzywilejowanym PAM/JIT w środowisku Microsoft Active Directory

W ramach usługi zostanie wykonana analiza istniejących kont, grup i uprawnień administracyjnych oraz opracowany model dostępu uprzywilejowanego zgodny z zasadą najmniejszych uprawnień i separacji obowiązków.

Środowisko administracyjne zostanie podzielone na warstwy bezpieczeństwa:

- Tier 0 – kontrolery domeny, Active Directory, AD CS/CA, konta Domain Admins i inne systemy kontrolujące tożsamość,
- Tier 1 – serwery członkowskie, systemy aplikacyjne, bazy danych, systemy backupu i infrastruktura serwerowa,
- Tier 2 – stacje robocze użytkowników i administracja urządzeniami końcowymi.

Dla administratorów zostaną przygotowane oddzielne konta administracyjne, których nie będzie można używać do codziennej pracy, poczty elektronicznej ani przeglądania Internetu. Dostęp do zasobów krytycznych będzie realizowany z wydzielonych i utwardzonych stanowisk administracyjnych PAW – Privileged Access Workstation lub równoważnych zabezpieczonych stanowisk administracyjnych.

W Active Directory zostanie uruchomiony mechanizm Privileged Access Management Feature, umożliwiający stosowanie czasowego członkostwa w grupach uprzywilejowanych z wykorzystaniem parametru Time-to-Live (TTL).

Dostęp administracyjny będzie mógł być nadawany wyłącznie na czas wymagany do wykonania określonego zadania, np. 30 lub 60 minut. Po upływie ustalonego czasu członkostwo użytkownika w grupie uprzywilejowanej automatycznie wygaśnie, bez konieczności ręcznego odbierania uprawnień.

Przykładowy model działania:

konto administratora → uwierzytelnienie → przyznanie uprawnienia JIT → wykonanie zadania → automatyczne wygaśnięcie uprawnienia

Wdrożone zostaną również mechanizmy:

- ograniczenia stałego członkostwa w grupach Domain Admins, Enterprise Admins i innych grupach uprzywilejowanych,
- separacji kont administracyjnych od kont użytkowników,
- kontroli logowania kont uprzywilejowanych do odpowiednich klas systemów,
- wykorzystania grup bezpieczeństwa AD do delegowania uprawnień,
- ochrony kont administracyjnych poprzez odpowiednie polityki GPO,
- wykorzystania grupy Protected Users i dodatkowych zabezpieczeń uwierzytelniania tam, gdzie jest to technicznie uzasadnione,
- zabezpieczenia lokalnych kont administratorów za pomocą Windows LAPS i automatycznej rotacji ich haseł,
- integracji uwierzytelniania administratorów z posiadaną infrastrukturą AD CS/CA oraz sprzętowymi kluczami bezpieczeństwa YubiKey/PIV, jeżeli zostaną wdrożone w ramach systemu uwierzytelniania,
- rejestrowania zdarzeń związanych z logowaniem i użyciem kont uprzywilejowanych oraz

przekazywania istotnych zdarzeń do systemu SIEM/Wazuh.

3.11. Wdrożenie Windows Application Control oraz Credential Guard

W ramach wdrożenia zostanie uruchomiony mechanizm Application Control pozwalający określić, jakie aplikacje, biblioteki, skrypty, instalatory i sterowniki mogą być wykonywane na chronionym systemie.

Dla dedykowanej stacji administracyjnej PAW zostanie przygotowana restrykcyjna polityka dopuszczająca uruchamianie wyłącznie zatwierdzonego oprogramowania niezbędnego do zarządzania infrastrukturą, w szczególności:

- narzędzi administracyjnych Microsoft RSAT,
- PowerShell i Windows Terminal,
- klienta RDP i SSH,
- narzędzi administracyjnych Active Directory, DNS, DHCP i GPO,
- narzędzi AD CS/CA,
- konsol zarządzania wirtualizacją, backupem i bezpieczeństwem,
- zatwierdzonej przeglądarki wykorzystywanej wyłącznie do lokalnych interfejsów administracyjnych,
- wskazanego przez Zamawiającego oprogramowania administracyjnego.

Polityka zostanie przygotowana zgodnie z modelem allow-listing, zgodnie z którym kod niespełniający określonych kryteriów zaufania nie będzie mógł zostać wykonany.

Wdrożenie zostanie przeprowadzone etapowo.

W pierwszej kolejności polityka zostanie uruchomiona w trybie Audit, w którym potencjalnie niedozwolone aplikacje i komponenty będą rejestrowane, ale nie będą jeszcze blokowane. Na podstawie zebranych zdarzeń zostanie przeprowadzona analiza kompatybilności i utworzona lista wymaganych wyjątków.

Po zakończeniu testów i zatwierdzeniu polityki system zostanie przełączony w tryb Enforcement, w którym nieautoryzowany kod będzie blokowany.

Polityki Application Control zostaną skonfigurowane tak, aby ograniczać możliwość uruchamiania m.in.:

- nieautoryzowanych plików wykonywalnych,
- skryptów i interpreterów mogących zostać wykorzystanych do wykonania złośliwego kodu,
- niezatwierdzonych instalatorów MSI,
- nieautoryzowanych bibliotek i komponentów,
- niebezpiecznych lub niezatwierdzonych sterowników.

Zdarzenia Application Control i Code Integrity będą rejestrowane i, w przypadku dostępności systemu SIEM, przekazywane do SIEM Zamawiającego.

3.11.2. Credential Guard

Na chronionych stacjach zostanie skonfigurowany i zweryfikowany mechanizm Credential Guard wykorzystujący Virtualization-Based Security (VBS) do odseparowania krytycznych danych uwierzytelniających od podstawowego systemu operacyjnego.

Credential Guard zabezpiecza m.in.:

- hashe haseł NTLM,
- bilety Kerberos TGT,
- wybrane poświadczenia domenowe,
- sekrety przetwarzane przez mechanizmy LSA.

Dane te są przechowywane w izolowanym środowisku bezpieczeństwa, dzięki czemu nie mogą być bezpośrednio odczytane przez standardowy proces LSASS ani przez złośliwe oprogramowanie działające w podstawowym systemie operacyjnym.

W ramach wdrożenia zostanie wykonana weryfikacja:

- obsługi VBS przez sprzęt,
- konfiguracji UEFI i Secure Boot,
- dostępności TPM 2.0,
- wymaganych funkcji procesora i wirtualizacji sprzętowej,
- zgodności wykorzystywanego oprogramowania administracyjnego,
- aktualnego stanu Credential Guard na chronionym urządzeniu.

Credential Guard zostanie wymuszony za pomocą centralnych polityk bezpieczeństwa, np. Group Policy, w sposób umożliwiający jego kontrolowane utrzymanie i audyt.

Dla dedykowanej stacji PAW mechanizm będzie stanowił dodatkową warstwę ochrony kont administracyjnych wykorzystywanych do zarządzania infrastrukturą Active Directory, serwerami i urządzeniami krytycznymi.

3.12.Wykonawca uruchomi system ITSM umożliwiający rejestrowanie i obsługę incydentów, zgłoszeń serwisowych i zmian dotyczących infrastruktury IT/OT. System zapewni role i uprawnienia, przypisywanie odpowiedzialności, priorytety, historię działań, powiązanie zgłoszeń z aktywami, powiadomienia oraz raportowanie. Zamawiający otrzyma dostęp administracyjny i możliwość eksportu danych.

3.13. Wykonawca wykona hardening urządzeń i systemów OT objętych projektem, z uwzględnieniem zaleceń producentów. Zakres obejmie ograniczenie zbędnych usług i dostępów, zarządzanie kontami, kopie konfiguracji oraz uzgodnione aktualizacje. Zdalny dostęp serwisowy będzie realizowany przez kontrolowany punkt dostępu z indywidualnymi kontami, MFA, ograniczeniem uprawnień i rejestrowaniem dostępnych zdarzeń sesji. Zmiany wymagają zatwierdzenia, planu powrotu i sprawdzenia działania procesu po ich wykonaniu.

3.14.2. System Web Application Firewall (WAF)

1. Zakres zamówienia

1.1. Objęcie subskrypcją minimum jedną domene/strefe internetową Zamawiającego.

1.2. Zapewnienie aktywności subskrypcji przez cały okres 36 miesięcy.

1.3. Przekazanie Zamawiającemu potwierdzenia zakupu, aktywacji lub przypisania subskrypcji.

1.4. Zapewnienie, że subskrypcja będzie dostępna do wykorzystania przez Zamawiającego w panelu administracyjnym producenta lub na koncie wskazanym przez Zamawiającego.

2. Minimalne wymagania funkcjonalne

Oferowana subskrypcja musi obejmować co najmniej:

4.1. Usługę DNS dla minimum dwóch domen/stref.
4.2. Usługę CDN.
4.3. Ochronę przed atakami DDoS.
4.4. WAF z regułami zarządzanymi.
4.5. Możliwość tworzenia własnych reguł bezpieczeństwa.
4.6. Obsługę SSL/TLS.
4.7. Panel administracyjny WWW.
4.8. Statystyki ruchu i zdarzeń bezpieczeństwa.
3. Wymagania dotyczące subskrypcji
3.1. Subskrypcja musi być aktywna przez okres 36 miesięcy od dnia aktywacji.
3.5. Wykonawca przekaże Zamawiającemu potwierdzenie aktywacji lub zakupu subskrypcji.
3.6. Subskrypcja musi pochodzić z legalnego kanału sprzedaży producenta lub autoryzowanego dystrybutora/partnera.
5. Warunki realizacji
5.3. W przypadku aktywacji na koncie Wykonawcy, Wykonawca zapewni Zamawiającemu możliwość korzystania z zakupionej subskrypcji przez pełny okres 36 miesięcy.
5.4. Wykonawca przekaże Zamawiającemu potwierdzenie okresu ważności subskrypcji.
6. Wymagania dotyczące bezpieczeństwa dostawcy i rozwiązania
Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:
6.1. Produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa.
6.2. Produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.

3.14.3. Oprogramowanie do centralnego zarządzania urządzeniami końcowymi – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja systemu klasy Endpoint Management /UEM, przeznaczonego do centralnego zarządzania komputerami i serwerami Zamawiającego.
System powinien być instalowany lokalnie w infrastrukturze Zamawiającego w modelu On-Premises.
Wymagania minimalne:
1. Liczba zarządzanych urządzeń: system musi umożliwiać zarządzanie co najmniej 20 urządzeniami końcowymi.
2. Model wdrożenia: system musi umożliwiać instalację w środowisku On-Premises, w infrastrukturze

Zamawiającego.

3. System operacyjny serwera: serwer zarządzający musi umożliwiać instalację na aktualnie wspieranym przez producenta systemie operacyjnym Microsoft Windows lub Windows Server.

4. Konsola administracyjna: dostęp do konsoli administracyjnej musi odbywać się za pomocą przeglądarki internetowej z wykorzystaniem szyfrowanego protokołu HTTPS.

5. Certyfikat TLS: system musi umożliwiać wykorzystanie własnego certyfikatu TLS dla konsoli administracyjnej.

6. Mechanizm zarządzania: zarządzanie urządzeniami musi odbywać się centralnie, z wykorzystaniem agentów lub równoważnego mechanizmu instalowanego na zarządzanych urządzeniach.

7. Kopia konfiguracji: system musi umożliwiać wykonywanie kopii zapasowej konfiguracji oraz danych systemu i ich późniejsze odtworzenie.

8. Uwierzytelnianie administratora: system musi umożliwiać uwierzytelnianie administratora z wykorzystaniem lokalnego repozytorium użytkowników lub Microsoft Active Directory.

9. MFA: system musi umożliwiać zastosowanie uwierzytelniania wieloskładnikowego MFA dla dostępu administracyjnego.

Zarządzanie urządzeniami

10. Obsługiwane systemy operacyjne: system musi obsługiwać aktualnie wspierane przez producenta wersje co najmniej:

- Microsoft Windows,
- Microsoft Windows Server,
- Linux,
- macOS.

11. Active Directory: system musi umożliwiać zarządzanie urządzeniami należącymi do domeny Microsoft Active Directory oraz urządzeniami pozostającymi poza domeną.

12. Urządzenia lokalne i zdalne: system musi umożliwiać zarządzanie urządzeniami pracującymi w sieci lokalnej oraz urządzeniami pracującymi zdalnie.

13. Optymalizacja dystrybucji: system powinien umożliwiać zastosowanie mechanizmu optymalizującego dystrybucję danych, aktualizacji i oprogramowania pomiędzy lokalizacjami lub przez łącza o ograniczonej przepustowości.

Zarządzanie aktualizacjami

14. Wykrywanie aktualizacji: system musi automatycznie wykrywać brakujące aktualizacje i poprawki bezpieczeństwa.

15. Wdrażanie aktualizacji: system musi umożliwiać centralne wdrażanie aktualizacji dla wspieranych systemów operacyjnych.

16. Aktualizacje aplikacji: system musi umożliwiać wdrażanie aktualizacji dla aplikacji producentów innych niż producent systemu operacyjnego.

17. Automatyzacja: system musi umożliwiać automatyzację procesu wdrażania aktualizacji według zdefiniowanego harmonogramu.

18. Grupa testowa: system musi umożliwiać utworzenie grupy testowej lub pilotażowej, na której poprawki mogą zostać zweryfikowane przed ich wdrożeniem na urządzenia produkcyjne.

19. Zatwierdzanie poprawek: system musi umożliwiać zatwierdzanie poprawek przed wdrożeniem ich w środowisku produkcyjnym.
20. Raportowanie aktualizacji: system musi umożliwiać raportowanie co najmniej:
- brakujących poprawek,
- stanu wdrożenia poprawek,
- urządzeń wymagających aktualizacji,
- urządzeń wymagających ponownego uruchomienia.

Dystrybucja i kontrola oprogramowania

21. Instalacja i deinstalacja: system musi umożliwiać centralną instalację i deinstalację oprogramowania na pojedynczym urządzeniu oraz grupie urządzeń.
22. Pakiety instalacyjne: system musi umożliwiać tworzenie lub definiowanie pakietów instalacyjnych.
23. Portal samoobsługowy: system musi umożliwiać udostępnianie użytkownikom zatwierdzonych aplikacji do samodzielnej instalacji poprzez portal samoobsługowy lub mechanizm równoważny.
24. Zdalne polecenia: system musi umożliwiać wykonywanie zdalnych poleceń lub skryptów administracyjnych.
25. PowerShell/CMD: dla systemów Microsoft Windows system musi umożliwiać wykonywanie skryptów lub poleceń PowerShell, CMD lub mechanizmu równoważnego.
26. Oprogramowanie niedozwolone: system musi umożliwiać wykrywanie wskazanego przez administratora oprogramowania niedozwolonego.
27. Działania naprawcze: system musi umożliwiać podjęcie działania naprawczego wobec oprogramowania niedozwolonego, w tym jego zdalną deinstalację lub zablokowanie.

Inwentaryzacja sprzętu i oprogramowania

28. Inwentaryzacja: system musi automatycznie prowadzić inwentaryzację sprzętu i oprogramowania zarządzanych urządzeń.
29. Inwentaryzacja sprzętu: system musi umożliwiać pozyskanie co najmniej informacji o:
- producencie urządzenia,
- modelu,
- systemie operacyjnym,
- procesorze,
- pamięci RAM,
- dyskach,
- interfejsach sieciowych,
- numerze seryjnym, jeżeli jest udostępniany przez urządzenie.

30. Inwentaryzacja oprogramowania: system musi umożliwiać inwentaryzację zainstalowanego oprogramowania wraz z informacją co najmniej o nazwie, wersji, producencie i urządzeniach, na których oprogramowanie jest zainstalowane.
31. Ewidencja licencji: system musi umożliwiać prowadzenie ewidencji licencji oprogramowania.
32. Wykorzystanie oprogramowania: system musi umożliwiać analizę wykorzystania lub stopnia wykorzystania wskazanego oprogramowania.
33. Gwarancje sprzętu: system powinien umożliwiać przechowywanie lub prezentowanie informacji

dotyczących gwarancji sprzętu.

Zdalna administracja

34. Zdalny dostęp: system musi umożliwiać bezpieczny zdalny dostęp do zarządzanych komputerów.

35. Zgoda użytkownika: system musi umożliwiać skonfigurowanie wymogu uzyskania zgody użytkownika na rozpoczęcie sesji zdalnej.

36. Transfer plików: system musi umożliwiać transfer plików pomiędzy stanowiskiem administratora a zarządzanym urządzeniem.

37. Rejestrowanie sesji: system powinien umożliwiać rejestrowanie lub nagrywanie sesji zdalnego dostępu.

38. Zdalne czynności administracyjne: system musi umożliwiać wykonywanie co najmniej podstawowych czynności administracyjnych bez konieczności uruchamiania pełnej sesji pulpitu zdalnego, w tym:

- wykonywanie poleceń,
- obsługę procesów,
- obsługę usług,
- operacje na plikach.

39. Zdalne sterowanie zasilaniem: system musi umożliwiać zdalne wyłączenie i ponowne uruchomienie zarządzanych urządzeń.

Kontrola USB i urządzeń peryferyjnych

40. Zarządzanie urządzeniami USB: system musi umożliwiać centralne zarządzanie dostępem do urządzeń USB oraz urządzeń peryferyjnych.

41. Kategorie urządzeń: system musi umożliwiać blokowanie lub zezwalanie na korzystanie z wybranych kategorii urządzeń.

42. Wyjątki: system musi umożliwiać definiowanie wyjątków dla określonych urządzeń lub klas urządzeń na podstawie dostępnych identyfikatorów sprzętowych.

43. Rejestrowanie użycia USB: system musi umożliwiać rejestrowanie lub raportowanie wykorzystania urządzeń USB.

Ochrona danych

44. Endpoint DLP: system musi posiadać mechanizm ochrony danych na urządzeniach końcowych klasy Endpoint DLP lub równoważny.

45. Polityki ochrony danych: system musi umożliwiać centralne definiowanie polityk ochrony danych.

46. Kanały przepływu danych: mechanizm ochrony danych musi umożliwiać kontrolę co najmniej wybranych kanałów przesyłania, kopiowania lub wynoszenia danych poza zarządzane urządzenie.

47. Zdarzenia DLP: system musi rejestrować zdarzenia naruszenia lub uruchomienia polityk ochrony danych.

48. Raportowanie DLP: system musi umożliwiać raportowanie zdarzeń związanych z ochroną danych.

BitLocker

49. Monitorowanie BitLocker: system musi umożliwiać centralne monitorowanie stanu szyfrowania BitLocker dla wspieranych urządzeń Microsoft Windows.

50. Zarządzanie szyfrowaniem: system musi umożliwiać zarządzanie konfiguracją szyfrowania

BitLocker lub równoważnego mechanizmu szyfrowania systemowego.

51. Odzyskiwanie: system musi zapewniać możliwość bezpiecznego przechowywania lub odzyskania informacji niezbędnych do odzyskania dostępu do zaszyfrowanego urządzenia.

Kontrola aplikacji i uprawnień

52. Kontrola aplikacji: system musi umożliwiać centralne definiowanie zasad kontroli uruchamiania aplikacji.

53. Listy aplikacji: system musi umożliwiać tworzenie list aplikacji dozwolonych lub niedozwolonych.

54. Blokowanie oprogramowania: system musi umożliwiać blokowanie wskazanego oprogramowania na zarządzanych urządzeniach.

55. Uprawnienia administracyjne: system powinien umożliwiać ograniczanie lokalnych uprawnień administracyjnych użytkowników i kontrolowane podnoszenie uprawnień dla wskazanych aplikacji lub zadań.

Zarządzanie podatnościami

56. Wykrywanie podatności: system musi umożliwiać wykrywanie podatności wynikających co najmniej z brakujących aktualizacji bezpieczeństwa.

57. Błędne konfiguracje: system powinien umożliwiać identyfikowanie błędnych konfiguracji lub innych podatności zarządzanych urządzeń.

58. Działania naprawcze: administrator musi mieć możliwość podjęcia działań naprawczych na podstawie wykrytych niezgodności, co najmniej poprzez:

- wdrożenie poprawki,
- usunięcie wskazanego oprogramowania,
- zmianę konfiguracji urządzenia.

Raportowanie

59. Raporty: system musi umożliwiać generowanie raportów obejmujących co najmniej:

- sprzęt,
- oprogramowanie,
- licencje,
- poprawki,
- stan aktualizacji,
- urządzenia USB,
- stan szyfrowania urządzeń.

60. Historia zadań: system musi przechowywać informacje o wykonanych zadaniach administracyjnych oraz ich statusie.

61. Eksport raportów: system powinien umożliwiać eksport raportów do co najmniej jednego powszechnie stosowanego formatu, np. CSV, XLSX lub PDF.

3.14.4. System ochrony poczty elektronicznej klasy Email Security

Przedmiotem zamówienia jest dostawa, wdrożenie, konfiguracja i utrzymanie systemu ochrony poczty elektronicznej przed phishingiem, spear-phishingiem, BEC, spoofingiem, malware,

ransomware, złośliwymi adresami URL i załącznikami oraz spamem.
Dopuszcza się model Secure Email Gateway, API-based Email Security albo model hybrydowy, w tym usługę chmurową, pod warunkiem spełnienia wymagań minimalnych.
Rozwiązanie musi obejmować wszystkich użytkowników/skrzynki na okres 36 miesięcy. Cena musi obejmować wszystkie licencje, subskrypcje, aktualizacje i składniki wymagane do działania opisanych funkcji.

3.14.4.1. Ochrona wiadomości i uwierzytelnienie nadawcy

System musi analizować co najmniej nadawcę i domenę, nazwę wyświetlaną, nagłówki, treść, URL, załączniki, reputację oraz wyniki SPF/DKIM/DMARC i wykrywać próby podszywania się pod użytkowników, osoby uprzywilejowane, kontrahentów i organizacje.
Wykonawca musi zweryfikować i, w zakresie wymaganym dla rozwiązania, skonfigurować SPF, DKIM i DMARC dla chronionych domen.

3.14.4.2. URL, załączniki i nieznane zagrożenia

System musi analizować adresy URL i załączniki z wykorzystaniem aktualizowanych mechanizmów reputacyjnych oraz co najmniej jednego mechanizmu umożliwiającego wykrywanie nieznanych zagrożeń, takiego jak analiza heurystyczna, behawioralna, uczenie maszynowe, sandboxing lub funkcjonalnie równoważna integracja z innym systemem bezpieczeństwa.
W przypadku wykrycia zagrożenia system musi umożliwiać odpowiednio do modelu: blokadę, kwarantannę, usunięcie wiadomości oraz powiadomienie administratora. Jeżeli model umożliwia analizę po dostarczeniu wiadomości, należy uruchomić funkcję post-delivery remediation.

3.14.4.3. Spam, kwarantanna i polityki

System musi automatycznie klasyfikować spam z wykorzystaniem co najmniej reputacji, analizy treści i nagłówków oraz reguł/heurystyki. Musi posiadać centralną kwarantannę z możliwością wyszukiwania, sprawdzenia przyczyny blokady, zwolnienia i usunięcia wiadomości oraz utworzenia reguły allow/block. Minimalna retencja kwarantanny: 14 dni.
Administrator musi mieć możliwość definiowania polityk co najmniej dla organizacji, domen, grup lub użytkowników oraz tworzenia list dozwolonych, blokowanych, wyjątków i własnych reguł bezpieczeństwa.

3.14.4.4. Wyszukiwanie, raportowanie i SIEM

System musi umożliwiać wyszukiwanie historii wiadomości co najmniej według nadawcy, odbiorcy, czasu, domeny, tematu, statusu i wyniku analizy. Historia musi być przechowywana minimum 30 dni albo przekazywana do SIEM zapewniającego taką retencję.
System musi raportować co najmniej phishing/BEC, malware, spam, wiadomości zablokowane i poddane kwarantannie oraz umożliwiać automatyczne przekazywanie zdarzeń bezpieczeństwa do SIEM przez udokumentowany mechanizm integracji.

3.14.4.5. Bezpieczeństwo zarządzania i chmura

System musi zapewniać szyfrowane zarządzanie, MFA dla administracji albo integrację z systemem tożsamości zapewniającym MFA, kontrolę uprawnień i rejestrację istotnych operacji

administracyjnych.
W przypadku rozwiązania chmurowego Wykonawca wskaże lokalizację/region przetwarzania danych, podstawowe kategorie danych oraz podmiot świadczący usługę. Wymagana dostępność usługi SaaS wynosi minimum 99,9% miesięcznie, z wyłączeniem uzgodnionych okien serwisowych.

3.14.4.6. Zakres uruchomienia

Wykonawca musi skonfigurować chronione domeny i użytkowników, polityki ochrony, SPF/DKIM/DMARC w wymaganym zakresie, mechanizmy phishing/BEC, ochronę URL i załączników, kwarantannę oraz integrację z SIEM.

3.14.5. Usługa typu Managed Intrusion Detection System (MIDS) IT/OT/ICS

3.14.5.1. Przedmiot i zakres usługi

Przedmiotem zamówienia jest świadczenie przez okres 36 miesięcy usługi MIDS zapewniającej bieżące zarządzanie, utrzymanie, strojenie i rozwój mechanizmów wykrywania zagrożeń dla infrastruktury IT oraz – w zakresie dostępnej telemetrii – OT/ICS.
Usługa musi wykorzystywać mechanizmy dostępne w UTM/NGFW, IDS/IPS, NDR, SIEM, systemach endpointowych, DNS Security i CTI. Nie wymaga się dostawy odrębnego SIEM, NDR ani kolejnego urządzenia IDS/IPS.
Zakres musi obejmować co najmniej sieci serwerowe, administracyjne, DMZ, VPN, połączenia z Internetem, komunikację IT–OT oraz systemy OT/ICS objęte telemetrią.

3.14.5.2. Zarządzanie detekcjami

Wykonawca musi zapewnić bieżący przegląd, aktualizację i weryfikację reguł i sygnatur, dostosowanie progów i poziomów istotności, uzasadnione wyjątki oraz – gdy jest to potrzebne – opracowanie własnych reguł lub korelacji.
Tuning musi obejmować analizę false positive i wpływu zmian na skuteczność detekcji. Nie dopuszcza się ograniczenia tuningu do wyłączania reguł generujących dużą liczbę alertów.
Mechanizmy detekcyjne muszą być dostosowywane do istotnych zmian środowiska, w tym nowych VLAN-ów, stref, serwerów, aplikacji, reguł UTM/NGFW i zmian w OT/ICS.

3.14.5.3. Minimalne klasy detekcji

Usługa musi utrzymywać i rozwijać detekcje co najmniej dla klas:

- próby wykorzystania podatności i exploity;
- malware oraz komunikacja Command and Control;
- IOC i Threat Intelligence;
- rekonesans i skanowanie;
- zagrożenia DNS;
- oznaki lateral movement w zakresie dostępnej telemetrii;
- niedozwolona lub nietypowa komunikacja IT–OT/ICS.

3.14.5.4. Threat Intelligence i stan źródeł

Wykonawca musi wykorzystywać wiarygodne i dostępne źródła Threat Intelligence, w tym źródła

producentów, publiczne źródła CTI, CERT/CSIRT oraz platformę CTI Zamawiającego, jeżeli jest dostępna.

Wykonawca musi monitorować dostępność źródeł telemetrii, poprawność przekazywania zdarzeń, aktualność treści detekcyjnych, integracje z SIEM oraz błędy mogące powodować utratę danych. Brak istotnej telemetrii musi być zgłaszany zgodnie z SLA.

3.14.5.5. Obsługa zdarzeń i reakcja

Istotne zdarzenia muszą być przekazywane do SIEM, SOC, MDR lub administratora zgodnie z architekturą Zamawiającego i zawierać co najmniej czas, źródło, cel, klasę wykrycia, poziom istotności i podstawowe informacje analityczne.

Jeżeli dostępne systemy umożliwiają reakcję automatyczną lub półautomatyczną, jej konfiguracja wymaga uzgodnienia z Zamawiającym. Działania mogące wpływać na OT/ICS lub dostępność usług nie mogą być wykonywane automatycznie bez zatwierdzonej procedury.

3.14.5.6. Walidacja i raportowanie

Wykonawca musi okresowo weryfikować skuteczność wybranych detekcji za pomocą bezpiecznych testów kontrolowanych, bez prowadzenia pełnych testów penetracyjnych, jeżeli są one przedmiotem odrębnej pozycji.

Nie rzadziej niż raz w miesiącu Wykonawca przekaże raport obejmujący stan źródeł, istotne wykrycia, false positive, wykonany tuning i zmiany reguł, problemy z telemetrią, wyniki walidacji oraz rekomendacje.

3.14.5.7. SLA i jakość usługi

Wykonawca przyjmuje zgłoszenia przez całą dobę. Obsługa zgłoszeń jest realizowana w dni robocze od 8:00 do 16:00. Maksymalny czas rozpoczęcia obsługi całkowitej utraty istotnej telemetrii wynosi 4 godziny robocze, problemu wysokiego — 8 godzin roboczych, a pozostałych problemów — 16 godzin roboczych. Bieg czasu poza godzinami obsługi rozpoczyna się lub jest kontynuowany w najbliższym okresie obsługi. Rozpoczęcie obsługi oznacza podjęcie diagnostyki przez osobę kompetentną, a nie automatyczne potwierdzenie zgłoszenia. SLA MIDS dotyczy działania mechanizmów detekcyjnych i nie stanowi SLA całodobowej obsługi incydentów przez SOC.

Zmiany reguł i konfiguracji muszą być ewidencjonowane. Działania blokujące lub ingerujące w infrastrukturę produkcyjną wymagają zgody Zamawiającego, z wyjątkiem działań wcześniej jednoznacznie zatwierdzonych w procedurze reagowania.

3.14.6. Usługa Managed Detection and Response (MDR)

3.14.6.1. Przedmiot i model świadczenia

Przedmiotem zamówienia jest świadczenie przez 12 miesięcy usługi MDR zapewniającej eksperckie wsparcie w pogłębionej analizie i reagowaniu na incydenty cyberbezpieczeństwa w środowisku IT oraz – w zakresie dostępnej telemetrii – OT/ICS.

W ramach ceny Wykonawca zapewni minimum 40 godzin pracy ekspertów MDR. Niewykorzystane godziny pozostają dostępne do końca okresu obowiązywania umowy. Wykonawca prowadzi

ewidencję wykorzystanej puli.

Usługa musi wykorzystywać posiadane lub wdrażane systemy Zamawiającego, w tym SIEM, endpoint security, UTM/NGFW, NDR/MIDS, Email Security, CTI, AD, DNS/DHCP, VPN i inne dostępne źródła. Nie wymaga się dostawy dodatkowej platformy bezpieczeństwa.

3.14.6.2. Uruchomienie i źródła danych

Na początku realizacji Wykonawca musi uzgodnić architekturę współpracy, dostępne źródła telemetryczne, kanały komunikacji, model eskalacji i autoryzacji działań oraz zasady ewidencji puli godzin.

Analiza MDR musi wykorzystywać odpowiednie do incydentu dane z dostępnych źródeł, bez wymagania, aby wszystkie pochodziły z jednego produktu lub producenta.

3.14.6.3. Analiza incydentów i threat hunting

Dla incydentu przekazanego do MDR Wykonawca musi, odpowiednio do dostępnych danych i charakteru zdarzenia, przeprowadzić analizę obejmującą potwierdzenie incydentu, identyfikację źródła i zaangażowanych zasobów, IOC, dostępną oś czasu, prawdopodobny wektor wejścia, oznaki lateral movement/persistence, zakres kompromitacji, wpływ oraz rekomendowane działania.

W ramach dostępnej puli godzin Wykonawca może prowadzić threat hunting na podstawie CTI, istotnego incydentu, informacji o nowym zagrożeniu albo zlecenia Zamawiającego. Dla TTP należy stosować MITRE ATT&CK lub równoważną metodykę, jeżeli dane pozwalają na wiarygodną klasyfikację.

3.14.6.4. Reakcja i analiza przyczyn

W przypadku potwierdzonego incydentu Wykonawca musi przygotować rekomendacje containment, obejmujące stosownie do sytuacji blokowanie IOC/komunikacji, działania na kontach i poświadczeniach, zmiany polityk bezpieczeństwa, ograniczenie komunikacji hosta albo inne środki ograniczające skutki incydentu.

Wykonawca może wspierać wykonanie działań containment, eradication i recovery po uzyskaniu wymaganej autoryzacji i w ramach dostępnej puli godzin. Działania wpływające na OT/ICS lub ciągłość procesów technologicznych wymagają uprzedniej zgody Zamawiającego.

Jeżeli zakres danych i dostępna pula godzin na to pozwalają, Wykonawca przeprowadzi analizę przyczyn źródłowych lub analizę powłamaniową w zakresie niezbędnym do określenia wektora wejścia, zakresu kompromitacji i środków ograniczających ryzyko ponownego wystąpienia.

3.14.6.5. Rozwój detekcji i procedur

Na podstawie analiz Wykonawca musi wskazywać luki detekcyjne oraz rekomendować nowe lub zmienione reguły, korelacje, IOC, progi i źródła telemetrii. Stałe wdrażanie i tuning mechanizmów detekcyjnych pozostają zakresem usługi MIDS.

MDR musi wykorzystywać obowiązujące procedury reagowania Zamawiającego i może, w ramach puli godzin, przygotować ich uzasadnione uzupełnienia lub aktualizacje.

3.14.6.6. Raportowanie, bezpieczeństwo dostępu i personel

Wykonawca będzie przekazywał raport kwartalny obejmujący wykonane czynności, analizowane

incydenty, najistotniejsze wnioski i rekomendacje oraz wykorzystaną i pozostałą pulę godzin. Dla istotnych incydentów, jeżeli zakres analizy to uzasadnia, Wykonawca przygotuje raport poincydentowy.

Dostęp Wykonawcy do infrastruktury musi odbywać się przez uzgodnione kanały, z MFA, indywidualnymi kontami, zasadą minimalnych uprawnień i możliwością identyfikacji wykonanych operacji.

Wykonawca musi zapewnić personel posiadający doświadczenie w analizie i reagowaniu na incydenty. Nie wymaga się certyfikatów konkretnego producenta.

3.14.7. Usługa Cyber Threat Intelligence (CTI) IT/OT/ICS/IIoT

3.14.7.1. Przedmiot i wykorzystanie istniejącego środowiska

Przedmiotem zamówienia jest świadczenie przez 12 miesięcy usługi Cyber Threat Intelligence dotyczącej zagrożeń istotnych dla środowiska IT, OT, ICS i IIoT Zamawiającego.

Usługa musi wykorzystywać przede wszystkim istniejące lub wdrażane systemy bezpieczeństwa i źródła informacji Zamawiającego, w tym UTM/NGFW, SIEM, NDR/MIDS, endpoint security, Email Security, DNS Security, WAF/CDN/DDoS, systemy podatności, OT/ICS, SOC i MDR.

Nie wymaga się zakupu odrębnej komercyjnej platformy TIP ani dodatkowych systemów bezpieczeństwa, jeżeli wymagany zakres może zostać osiągnięty przy wykorzystaniu istniejących lub już licencjonowanych źródeł i mechanizmów.

3.14.7.2. Profil informacyjny i źródła CTI

Na początku realizacji Wykonawca wspólnie z Zamawiającym określi Profil CTI obejmujący technologie i systemy Zamawiającego, zasoby publicznie dostępne i krytyczne, tożsamość, VPN, pocztę, infrastrukturę sieciową, OT/ICS, kluczowych dostawców oraz zagrożenia sektorowe dotyczące wodociągów i infrastruktury krytycznej.

Wykonawca musi korzystać z kombinacji wiarygodnych źródeł obejmujących co najmniej informacje producentów wykorzystywanych technologii, CERT/CSIRT, źródła podatności i aktywnych exploitów, źródła branżowe i reputacyjne oraz informacje o kampaniach malware/ransomware/phishing i zagrożeniach OT/ICS.

3.14.7.3. Zakres danych, weryfikacja i priorytetyzacja

Usługa musi obejmować co najmniej IOC (IP, domeny, URL, hashe i inne przydatne identyfikatory), podatności/CVE, TTP oraz informacje o kampaniach i zagrożeniach.

Wykonawca musi zapewnić weryfikację źródła, deduplikację, wzbogacanie, ocenę aktualności, wiarygodności i istotności dla Zamawiającego. Nie dopuszcza się automatycznego blokowania wszystkich IOC pochodzących z niezweryfikowanych źródeł.

Najwyższy priorytet należy nadawać zagrożeniom aktywnie wykorzystywanym, dotyczącym technologii Zamawiającego, ransomware, infrastruktury wodociągowej i OT/ICS, urządzeń brzegowych, systemów dostępnych z Internetu oraz przejęcia tożsamości uprzywilejowanych.

Informacje o TTP należy mapować do MITRE ATT&CK oraz MITRE ATT&CK for ICS albo równoważnych modeli, jeżeli dostępne dane umożliwiają wiarygodne przypisanie.

3.14.7.4. *Integracja i operacyjne wykorzystanie*

CTI musi umożliwiać operacyjne wykorzystanie informacji przez SIEM, UTM/NGFW, NDR/MIDS, SOC i MDR oraz – w zakresie funkcji dostępnych w tych systemach – Email Security i endpoint security.

Integracja z SIEM musi umożliwiać co najmniej wyszukiwanie IOC w logach, wzbogacanie zdarzeń, wykorzystanie IOC w detekcjach i korelacjach oraz przekazywanie informacji o wykryciu IOC. Dopuszcza się API, pliki, listy dynamiczne, skrypty, JSON/CSV, STIX/TAXII lub inny udokumentowany mechanizm.

Informacje CTI przekazane do UTM/NGFW, MIDS/NDR lub innych systemów muszą być wykorzystywane w zakresie obsługiwanym przez posiadane rozwiązania; nie wymaga się zastępowania natywnych baz producenta zewnętrznym feedem.

3.14.7.5. *OT/ICS, podatności i alerty*

Usługa musi uwzględniać zagrożenia dotyczące OT/ICS, w tym podatności urządzeń przemysłowych i HMI/SCADA, zagrożenia dla urządzeń sieciowych OT, malware przemysłowy, zdalny dostęp, kompromitację dostawców i łańcucha dostaw oraz kampanie dotyczące infrastruktury krytycznej.

CTI musi wspierać priorytetyzację podatności, ze szczególnym uwzględnieniem podatności aktywnie wykorzystywanych, posiadających publiczny exploit, dotyczących technologii Zamawiającego, systemów dostępnych z Internetu, urządzeń bezpieczeństwa i OT/ICS.

W przypadku zweryfikowanego, istotnego zagrożenia bezpośrednio dotyczącego technologii Zamawiającego Wykonawca musi przekazać alert zawierający odpowiednio opis, poziom istotności, dotknięte technologie, znane IOC/TTP, informacje o podatnościach i rekomendowane działania. Alert krytyczny musi zostać przekazany bez zbędnej zwłoki po weryfikacji.

3.14.7.6. *Produkty CTI i formaty wymiany*

Wykonawca musi dostarczać informacje operacyjne dla administratorów, SOC, MDR i MIDS oraz raport CTI nie rzadziej niż raz w miesiącu. Raport musi zawierać ocenę znaczenia zagrożeń dla środowiska Zamawiającego, a nie jedynie zestawienie publicznie dostępnych informacji.

Jeżeli dane CTI są przekazywane maszynowo, musi być obsługiwany co najmniej jeden powszechnie stosowany format lub interfejs umożliwiający automatyczne wykorzystanie danych. Informacje podlegające ograniczeniom udostępniania muszą być oznaczane i obsługiwane zgodnie z TLP lub równoważnym mechanizmem stosowanym przez źródło.

Jeżeli źródła CTI udostępniają reguły detekcyjne, mogą być one przekazywane w formatach właściwych dla systemów Zamawiającego, bez obowiązku tworzenia reguły dla każdego IOC.

3.14.8. Świadczenie wsparcia technicznego Systemu do cyberbezpieczeństwa

1. Okres i zasady świadczenia wsparcia

1.1. Wykonawca zobowiązany jest do świadczenia usług wsparcia technicznego Systemu do cyberbezpieczeństwa przez okres 12 miesięcy od dnia podpisania końcowego protokołu odbioru.

1.2. Wynagrodzenie za świadczenie usług wsparcia technicznego przez cały wymagany okres zawarte jest w cenie oferty. Zamawiający nie ponosi z tego tytułu dodatkowych opłat.

1.3. Każda aktualizacja lub rozbudowa Systemu wykonana w ramach przedmiotu zamówienia jest automatycznie objęta wsparciem technicznym na warunkach określonych w niniejszym rozdziale.

1.4. Okresy gwarancji, licencji i subskrypcji innych elementów zamówienia pozostają zgodne z wymaganiami określonymi dla poszczególnych pozycji OPZ.

2. Klasyfikacja nieprawidłowości

Na potrzeby świadczenia usług wsparcia technicznego przyjmuje się następujące kategorie nieprawidłowości:

Kategoria	**Opis**	**Przykład skutku**
Awaria	Krytyczna niezgodność z dokumentacją powodująca zatrzymanie działania Systemu lub ryzyko utraty spójności danych.	Brak dostępu do modułu dashboard, groźba uszkodzenia bazy danych.
Błąd	Zakłócenie działania Systemu inne niż Awaria.	Funkcja eksportu PDF zwraca błąd, ale praca Systemu trwa.
Wada	Niedogodność nieograniczająca kluczowych procesów Systemu.	Literówka w interfejsie, nieoptymalny raport.

3. Zgłaszanie i klasyfikacja nieprawidłowości

3.1. Zgłoszenia przekazywane są przez portal Service Desk lub formularz mailowy.

3.2. Zamawiający wskazuje kategorię zgłaszanej nieprawidłowości. Wykonawca potwierdza lub koryguje kategorię w odpowiedzi zwrotnej.

4. Poziomy SLA

Wykonawca zobowiązany jest do zachowania następujących maksymalnych czasów reakcji i usunięcia nieprawidłowości:

Kategoria	**Maksymalny czas reakcji**	**Maksymalny czas usunięcia**
AWARIA	8 godzin	2 dni robocze od przyjęcia zgłoszenia
BŁĄD	2 dni robocze	7 dni roboczych od przyjęcia zgłoszenia
WADA	5 dni roboczych	20 dni roboczych od przyjęcia zgłoszenia

5. Zakres usług wsparcia technicznego

5.1. W ramach wynagrodzenia za realizację przedmiotu zamówienia Wykonawca świadczy usługi wsparcia technicznego bez dodatkowych opłat.

5.2. Zakres usług obejmuje w szczególności:

a) usuwanie Awarii, Błędów i Wad wynikających z:

- błędów w Systemie lub pakietach aktualizacyjnych,
- błędów dokumentacji,
- wadliwego wykonania usług wdrożeniowych;

b) wykonywanie korekt konfiguracji Systemu po aktualizacjach producenta;

c) rekonfigurację lub reinstalację Systemu po awarii sprzętu w terminie 72 godzin od zgłoszenia przez Zamawiającego gotowości infrastruktury do odtworzenia;

d) zdalne lub wykonywane na miejscu usuwanie usterek, stosownie do charakteru nieprawidłowości;
e) świadczenie pomocy technicznej (Helpdesk) w godzinach pracy Zamawiającego, z możliwością zgłaszania problemów przez portal internetowy;
f) wykonywanie czynności administracyjnych i naprawczych dotyczących baz danych, w szczególności naprawy uszkodzeń, aktualizacji struktur oraz przeciwdziałania duplikacji danych i utracie ich integralności.

5.3. Wykonawca realizuje czynności naprawcze w zakresie, w jakim posiada niezbędne uprawnienia techniczne i prawne do ingerencji w oprogramowanie, jego konfigurację lub kod źródłowy.

5.4. W przypadku nieprawidłowości dotyczących komponentów zewnętrznych, do których Wykonawca nie posiada prawa ingerencji w kod źródłowy, zobowiązany jest do przeprowadzenia diagnostyki, zastosowania dostępnych działań naprawczych oraz współpracy z producentem lub dostawcą komponentu w zakresie wynikającym z warunków gwarancji, licencji i wsparcia.

3.15. System SIEM dla obszaru IT i OT – S04 i U39

Opis wymagań minimalnych
Wymagania funkcjonalne 1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL. 2. System musi pracować w oparciu o architekturę Linux. 3. System musi mieć możliwość centralnego zbierania i zarządzania logami, w tym instalacji i rejestracji agentów (max. 200) na wskazanych przez Zamawiającego endpointach (w tym systemach operacyjnych Windows, Linux, AIX itp.). 4. System działać w trybie zbliżonym do rzeczywistego. 5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu. 6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu. 7. System musi zapewniać efektywną obsługę co najmniej 2500 EPS lub 50 GB danych dziennie. 8. System musi zapewniać retencję danych w okresie minimum 365 dni. 9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu. 10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska. 11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). 12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności powinno odbywać się bez konieczności restartu działającego systemu. 13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji.

14. System musi zapewniać buforowanie agregowanych danych na okres minimum 1 dnia w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie po przywróceniu pełnej sprawności systemu.
15. Komunikacja pomiędzy wszystkimi komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokół TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
18. Interfejs musi posiadać angielską lub polską wersję językową.
19. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project).
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius.
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
23. System musi wspierać mechanizm logowania typu Single Sign On.
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
26. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełną historię operacji, realizowanych zapytań, zmian uprawnień.
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
29. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
30. System musi zapewniać wizualizację danych w postaci oryginalnych logów, list, wykresów i diagramów.
31. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
32. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
33. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu XLSX, CSV m.in. w celu analizy wyników działania reguł korelacyjnych.
34. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

35. Syslog, WEF, Flat file, Event log, WMI, XML, JSON, JDBC/ODBC, CSV, Email, jak również musi pozwalać na implementację innych formatów tym Sysmon w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
36. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
37. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie, w jakiej ten log został przesłany do Systemu, tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
38. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe; ponadto musi umożliwiać integrację z istniejącym u Zamawiającego sieciowym systemem wykrywania włamań (NIDS) w celu usprawnienia monitorowania i inspekcji ruchu sieciowego.
39. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
40. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
41. System musi posiadać predefiniowany zestaw parserów zdarzeń.
42. System musi posiadać funkcjonalność Bad IP i Domain Reputation, umożliwiającą porównywanie adresów IP oraz domen z bazami reputacyjnymi na podstawie automatycznie aktualizowanych źródeł OSINT (m.in. CBD LIST, DNSBL, zbiory baz niskiej reputacji IP) oraz wskaźników kompromitacji (IOC).
43. System musi mieć funkcjonalność sprawdzania, czy dane uwierzytelniające ujawnione zostały w publicznych bazach wycieków.
44. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
45. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
46. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
47. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzne procedury bezpieczeństwa.
48. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
49. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
50. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego, dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowanie alarmów.
51. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
52. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.

53. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
    - Wykrycia dowolnej treści w logach,
    - Wykrycia wystąpienia wartości pola na wybranej liście,
    - Wykrycia niewystępowania wartości pola na wybranej liście,
    - Wykrycia zmiany jednego z kilku pól,
    - Wykrycia zdarzeń występujących z zadaną częstotliwością,
    - Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
    - Wykrycia zaniku Wiadomości,
    - Wykrycia nowej wartości pola w zadanym okresie czasu,
    - Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności.
54. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów.
55. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
56. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.
57. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności.
58. System umożliwia konfigurację automatycznych akcji, które są wykonywane na monitorowanych systemach
    w przypadku detekcji zagrożenia wskazanego w regule (moduł Active Response). Musi istnieć możliwość tworzenia i modyfikowania skryptów dostosowanych do środowiska Zamawiającego, np. blokowanie złośliwego ruchu, usuwanie plików, blokowanie kont użytkowników.
59. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
60. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
61. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
62. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz zarządzanie nimi z poziomu konsoli użytkownika. Niezależnie od tego, musi istnieć możliwość przygotowania odpowiednich procedur i wdrożenia mechanizmu backupu oraz odtwarzania konfiguracji oprogramowania, uwzględniającego środowisko Zamawiającego.
63. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
64. Mechanizm archiwizacji musi umożliwiać przywracanie danych do systemu celem analizy online.

65. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
66. System musi umożliwiać zbieranie i analizę pełnego ruchu sieciowego (warstwy modelu ISO OSI od L2 do L7) oraz analizę formatu Netflow, a także integrację informacji z posiadanym przez Zamawiającego NIDS w celu rozszerzonej detekcji włamań.
67. System musi umożliwiać analize zachowań i logów z różnych źródeł (np. systemowych, aplikacyjnych, firewalli) oraz wykrywać wzorce ataków na poziomie infrastruktury, systemu i aplikacji.
68. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
69. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
70. Wsparcie musi być realizowane w języku polskim przez dedykowanych inżynierów.
71. Support musi być świadczony w formule minimum 8/5.
72. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), reputacji plików i hashy, zainfekowanych plików, adresy domen, adresy URL, a następnie automatycznego przeszukiwania wśród zgromadzonych zdarzeń w wyznaczonym czasie.
73. System musi umożliwiać mapowanie się na MITRE ATT&CK.
74. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych oraz umożliwiać przeprowadzenie audytu, modyfikacji i optymalizacji reguł OSSEC na potrzeby środowiska Zamawiającego.
75. System musi dostarczać funkcjonalność badania integralności plików i rejestrów na monitorowanych hostach (FIM), w tym monitorowanie zmian w plikach i katalogach, uprawnień dostępu do pliku, atrybutów plików oraz sum kontrolnych MD5 i SHA1. Dodatkowo system musi wspierać integrację z VirusTotal i frameworkiem Yara, by wspomagać aktywne skanowanie plików pod kątem malware i złośliwego kodu.
76. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark. (Security Configuration Assessment – SCA)
77. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
78. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkitów, wykrywania ukrytych procesów, plików i portów. Odpowiada za to m.in. moduł „Rootcheck", który ma identyfikować podejrzane binaria i anomalie świadczące o złośliwym oprogramowaniu.
79. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux
    i Windows (Vulnerability Detection) z możliwością aktualizacji bazy CVE Wazuh w trybie offline.
80. System powinien dodatkowo oferować moduł Extended Detection and Response (XDR), odpowiedzialny za zbieranie rozszerzonych danych telemetrycznych z punktów końcowych, urządzeń sieciowych,

środowisk chmurowych i innych źródeł, celem ujednoliconego monitorowania oraz zaawansowanej ochrony. 81. System musi umożliwiać obsługę i optymalizację scenariuszy Active Response, w tym tworzenia nowych skryptów reagowania i niwelowania zagrożeń bezpieczeństwa zgodnie z potrzebami Zamawiającego.

3.15.1. Identity Threat Detection and Response (ITDR)

Przedmiotem zamówienia jest wdrożenie, konfiguracja i uruchomienie mechanizmów klasy Identity Threat Detection and Response (ITDR), służących do identyfikacji, monitorowania, analizy i ograniczania zagrożeń związanych z tożsamością, uwierzytelnianiem, uprawnieniami oraz konfiguracją Active Directory Zamawiającego.
Rozwiązanie może wykorzystywać funkcjonalności posiadanego lub wdrażanego systemu SIEM/XDR oraz natywne mechanizmy systemów Windows Server i Active Directory.
Cena musi obejmować wszystkie prace wdrożeniowe, konfiguracje, integracje i komponenty niezbędne do realizacji wymaganego zakresu.
2. Analiza bezpieczeństwa Active Directory
Wykonawca przeprowadzi podstawową analizę bezpieczeństwa Active Directory, obejmującą co najmniej:

- identyfikację kont i grup uprzywilejowanych oraz istotnych kont usługowych;
- weryfikację członkostwa w grupach administracyjnych i nadmiernych uprawnień;
- przegląd podstawowych delegacji, istotnych uprawnień ACL oraz konfiguracji GPO;
- identyfikację nieaktywnych, nieużywanych lub nieprawidłowo zabezpieczonych kont;
- weryfikację wybranych ustawień bezpieczeństwa domeny, zasad haseł, blokowania kont oraz konfiguracji audytu;
- identyfikację istotnych nieprawidłowości mogących prowadzić do nadużycia uprawnień lub przejęcia kont administracyjnych.

Analiza zostanie przeprowadzona z wykorzystaniem natywnych narzędzi administracyjnych Windows Server, Active Directory, GPO i PowerShell, bez obowiązku wdrażania odrębnych narzędzi audytowych.
3. Analiza bezpieczeństwa AD CS
Jeżeli Zamawiający wykorzystuje Active Directory Certificate Services (AD CS), Wykonawca przeprowadzi podstawową analizę konfiguracji urzędu certyfikacji, istotnych szablonów certyfikatów oraz uprawnień do ich wydawania i zarządzania.
Analiza musi umożliwiać identyfikację podstawowych nieprawidłowości mogących prowadzić do nieuprawnionego wydawania certyfikatów, podszywania się pod użytkowników lub nadużycia uprawnień.
W przypadku braku AD CS zakres ten nie ma zastosowania.

4. Monitorowanie i detekcja zagrożeń tożsamościowych

Wykonawca skonfiguruje lub zweryfikuje mechanizmy audytu Windows oraz zbieranie i analizę zdarzeń Active Directory w systemie SIEM/XDR.

Zakres musi obejmować co najmniej:

- nieudane logowania, blokady kont i powtarzające się próby uwierzytelniania;
- tworzenie, usuwanie, włączanie i wyłączanie kont użytkowników;
- zmiany członkostwa w grupach uprzywilejowanych;
- istotne zmiany właściwości kont administracyjnych, uprawnień i GPO;
- podejrzane działania administracyjne oraz zdarzenia dotyczące kontrolerów domeny;
- zdarzenia mogące wskazywać na nadużycie tożsamości, próby eskalacji uprawnień lub wykorzystanie przejętych poświadczeń, w zakresie dostępnej telemetrii.

Wykonawca zapewni konfigurację niezbędnych zasad audytu, reguł detekcyjnych, korelacji i poziomów istotności alertów, z uwzględnieniem ograniczania fałszywych alarmów.

5. Reagowanie na zagrożenia i integracja z SIEM/XDR

Rozwiązanie musi zapewniać generowanie alertów, ich klasyfikację, prezentację w centralnym interfejsie SIEM/XDR oraz powiadamianie administratora o istotnych zagrożeniach tożsamościowych. Dopuszcza się wykorzystanie dostępnych mechanizmów Active Response, skryptów PowerShell oraz natywnych funkcji administracyjnych Active Directory w zatwierdzonych scenariuszach reagowania.

Nie wymaga się automatycznego blokowania kont, modyfikowania uprawnień ani izolowania kontrolerów domeny. Działania mogące wpływać na dostępność usług lub kont uprzywilejowanych muszą wymagać uprzedniego zatwierdzenia przez Zamawiającego.

Jeżeli posiadane systemy nie zapewniają informacji wystarczających do wykonania wymaganej analizy, Wykonawca może zastosować dodatkowe narzędzia pomocnicze, pod warunkiem że ich użycie zostanie uzgodnione z Zamawiającym, nie naruszy bezpieczeństwa danych i nie spowoduje obowiązku zakupu dodatkowej licencji po zakończeniu realizacji. Koszt takich narzędzi musi być ujęty w cenie oferty.

1. Narzędzia pomocnicze

Jeżeli posiadane systemy nie zapewniają informacji wystarczających do wykonania wymaganej analizy, Wykonawca może zastosować dodatkowe narzędzia pomocnicze, pod warunkiem że ich użycie zostanie uzgodnione z Zamawiającym, nie naruszy bezpieczeństwa danych i nie spowoduje obowiązku zakupu dodatkowej licencji po zakończeniu realizacji. Koszt takich narzędzi musi być ujęty w cenie oferty.

3.15.2. Konfiguracja i uruchomienie funkcjonalności Extended Detection and Response (XDR) w istniejącej platformie SIEM/XDR

Przedmiotem zamówienia jest konfiguracja, rozbudowa i integracja funkcjonalności klasy Extended Detection and Response (XDR) w istniejącej platformie SIEM eksploatowanej przez Zamawiającego.

3.15.2.1. Telemetria i integracje

Wykonawca musi skonfigurować lub zweryfikować zbieranie i wykorzystywanie telemetryki z endpointów, Active Directory oraz uzgodnionych systemów bezpieczeństwa. Zakres musi

obejmować co najmniej zdarzenia bezpieczeństwa i systemowe, informacje o hoście i użytkowniku, inventory sprzętu i oprogramowania, wybrane zdarzenia procesowe oraz zmiany plików i konfiguracji. Platforma musi wykorzystywać istotne źródła dostępne u Zamawiającego, w tym – w zakresie, w jakim dostarczają użytecznej telemetryki – UTM/NGFW, IDS/IPS, endpoint security, Windows/Linux, AD, urządzenia sieciowe, Email Security, NDR/MIDS i CTI. Integracja może być realizowana dowolnym udokumentowanym mechanizmem obsługiwanym przez systemy źródłowe i docelowe.

3.15.2.2. Detekcja, korelacja i tuning

Wykonawca musi skonfigurować i dostosować reguły detekcyjne, parsowanie/dekodowanie zdarzeń, korelacje oraz poziomy istotności alertów, w tym własne reguły niezbędne dla środowiska Zamawiającego.

Detekcje muszą obejmować co najmniej zagrożenia dotyczące tożsamości, endpointów, zmian konfiguracji, podatności, zdarzeń sieciowych i IOC. Istotne detekcje należy mapować do MITRE ATT&CK lub równoważnej bazy wiedzy TTP, jeżeli charakter zdarzenia pozwala na wiarygodne przypisanie.

Tuning musi obejmować analizę false positive, dostosowanie progów i warunków, uzasadnione wyjątki oraz poziomy istotności. Nie dopuszcza się ograniczenia tuningu do masowego wyłączania reguł.

3.15.2.3. FIM, ocena konfiguracji i podatności

Wykonawca musi skonfigurować lub zweryfikować:

- File Integrity Monitoring dla uzgodnionych plików, obiektów i – dla Windows – uzasadnionych elementów rejestru;
- Security Configuration Assessment umożliwiający identyfikację zgodności/niezgodności i wykorzystanie uznanych benchmarków;
- Vulnerability Detection oparty na inventory oprogramowania, wersjach komponentów i aktualizowanej bazie podatności, z identyfikacją hosta, komponentu, podatności i jej istotności.

Vulnerability Detection nie zastępuje aktywnego skanera podatności.

3.15.2.4. IOC, Threat Intelligence i threat hunting

Platforma musi wykorzystywać IOC i kontekst CTI dostępny u Zamawiającego do wzbogacania, detekcji, korelacji i wyszukiwania zdarzeń. Nie wymaga się budowy odrębnej platformy CTI ani zakupu dodatkowych feedów w ramach tej pozycji.

Wykonawca musi udostępnić i skonfigurować funkcjonalność analitycznego przeszukiwania zdarzeń i alertów według co najmniej czasu, hosta, użytkownika, adresu IP, reguły, poziomu alertu, kategorii zdarzenia i przypisanej techniki MITRE. Regularny threat hunting wykonywany przez analityków nie wchodzi w zakres tej pozycji.

3.15.2.5. Active Response

Wykonawca musi skonfigurować lub zweryfikować mechanizm Active Response umożliwiający automatyczne lub półautomatyczne wykonanie bezpiecznych reakcji po określonym alercie, w tym co najmniej uruchomienie skryptu oraz wywołanie dostępnego mechanizmu sieciowego lub

integracyjnego/API.

Reakcje wpływające na użytkownika lub usługę wymagają klasyfikacji i, odpowiednio do ryzyka, zatwierdzenia operatora. Bez zatwierdzonej procedury nie dopuszcza się automatycznego blokowania kont uprzywilejowanych, odcinania kontrolerów domeny, izolowania systemów krytycznych ani blokowania systemów OT/ICS. Jeżeli mechanizm to umożliwia, reakcje blokujące należy konfigurować jako czasowe.

3.15.2.6. Dashboardy i przypadki użycia

Wykonawca musi skonfigurować lub dostosować centralne widoki umożliwiające analizę istotnych alertów, źródeł/agentów, FIM, SCA, podatności, wyników threat huntingu i klasyfikacji MITRE ATT&CK.

Wdrożenie musi obejmować działające przypadki użycia co najmniej dla klas: Identity, Endpoint, Vulnerability, Configuration, Network oraz Threat Intelligence. Nie wymaga się sztucznej minimalnej liczby reguł w każdej klasie, jeżeli nie wynika ona z potrzeb środowiska.

3.15.2.7. Bezpieczeństwo administracji

Dostęp administracyjny musi być realizowany przy użyciu indywidualnych kont, zasady minimalnych uprawnień, rejestrowania istotnych działań oraz MFA, jeżeli wykorzystywany mechanizm uwierzytelniania umożliwia jego zastosowanie.

3.15.2.8. Badanie i zarządzanie podatnościami oraz *Testy bezpieczeństwa infrastruktury IT/OT/ICS/IIoT – U02*

Wykonawca zapewni w ramach ceny zamówienia instalację i konfigurację aktywnego skanera podatności infrastruktury IT. Dopuszcza się rozwiązanie open source lub komercyjne. Skaner musi umożliwiać aktualizację bazy podatności, skanowanie uwierzytelnione i nieuwierzytelnione, identyfikację podatności oraz sporządzanie raportów. Rozwiązanie zostanie przekazane Zamawiającemu wraz z dostępem administracyjnym i instrukcją eksploatacji.

Wykonawca przeprowadzi testy bezpieczeństwa infrastruktury IT/OT/ICS/IIoT objętej zamówieniem, obejmujące ocenę podatności, konfiguracji, segmentacji sieci i dostępu zdalnego. Przed rozpoczęciem badań przedstawi do zatwierdzenia plan określający zasoby, metody, harmonogram, ograniczenia i zasady przerwania testów.

W środowisku OT pierwszeństwo mają metody pasywne i analiza konfiguracji. Aktywne skanowanie OT wymaga uprzedniego zatwierdzenia przez Zamawiającego, uwzględnienia zaleceń producentów oraz uzgodnienia okna serwisowego.

Wykonawca przekaże raport zawierający wykaz przebadanych zasobów, zastosowane metody, wykryte podatności, ocenę ryzyka i zalecenia. Usunie niezgodności dotyczące dostarczonych lub skonfigurowanych przez siebie rozwiązań i przeprowadzi retest. Wyniki będą zawierały status działań naprawczych oraz wskazanie ryzyk pozostających po zakończeniu prac.

3.15.3. Wdrożenie warstwy detekcji i reakcji na zagrożenia sieciowe klasy Network Detection and Response (NDR)

Przedmiotem zamówienia jest wdrożenie i uruchomienie warstwy funkcjonalnej Network Detection

and Response (NDR), obejmującej wykrywanie, analizę, korelację i obsługę zagrożeń sieciowych w zakresie funkcjonalności określonych w niniejszym opisie, z wykorzystaniem dostępnych źródeł telemetrii oraz komponentów infrastruktury Zamawiającego.). Rozwiązanie może być realizowane jako odrębne oprogramowanie, moduł SIEM/XDR, moduł UTM/NGFW albo zestaw zintegrowanych komponentów wykorzystujących dostępne źródła telemetrii, w szczególności UTM/NGFW, SIEM, systemy endpointowe, AD, DNS/DHCP, CTI i inwentaryzację aktywów.

Nie wymaga się odrębnego fizycznego urządzenia lub pasywnego sensora NDR, jeżeli wymagane funkcjonalności zostaną zapewnione przez oprogramowanie i współdziałające komponenty środowiska Zamawiającego. Wykonawca musi jednoznacznie wskazać komponent lub komponenty realizujące O14 oraz zapewnić wszystkie wymagane licencje, subskrypcje, moduły, konfigurację i integrację.

2. Widoczność sieciowa i segmentacja

Wykonawca musi przeanalizować widoczność komunikacji w sieciach użytkowników, serwerowych, administracyjnych, DMZ, VPN oraz IT/OT/ICS, w tym ruch między VLAN-ami i strefami bezpieczeństwa oraz komunikację z Internetem.

Analiza musi wskazać kierunki komunikacji widoczne i niewidoczne dla dostępnych mechanizmów, ze szczególnym uwzględnieniem użytkownicy–serwery, IT–OT, DMZ–LAN, VPN–zasoby wewnętrzne, administracja–systemy krytyczne oraz ruchu wewnątrz tego samego segmentu. Wprowadzenie zmian w routingu, segmentacji lub politykach wymaga akceptacji Zamawiającego.

3. Telemetria, UTM/NGFW i SIEM

Warstwa NDR musi wykorzystywać dostępne w UTM/NGFW informacje dotyczące ruchu, aplikacji, IPS, malware/spyware, C2, DNS, analizy plików, Threat Intelligence, użytkowników, aktywów oraz ruchu dozwolonego i blokowanego.

Wykonawca musi zapewnić przekazywanie do SIEM danych niezbędnych dla detekcji NDR oraz ich poprawne parsowanie, normalizację kluczowych pól, wyszukiwanie, korelację i spójność znaczników czasu.

Warstwa NDR musi wykorzystywać informacje o aktywach z dostępnych źródeł, bez wymagania pełnego profilowania urządzeń przez jeden produkt.

4. Minimalne klasy detekcji NDR

Wykonawca musi skonfigurować i zweryfikować detekcje obejmujące co najmniej:

- Command and Control oraz komunikację z IOC o złej reputacji;
- próby wykorzystania podatności i zdarzenia IPS;
- malware oraz korelację zdarzeń sieciowych z endpointowymi, jeżeli dane są dostępne;
- zagrożenia DNS, w tym komunikację z niebezpiecznymi domenami;
- rekonesans i skanowanie;
- oznaki ruchu lateralnego w zakresie dostępnej telemetrii;
- naruszenia komunikacji i nietypowe zdarzenia pomiędzy strefami IT i OT/ICS.

Każda detekcja musi posiadać określone źródło danych, poziom istotności, warunek uruchomienia i zalecaną reakcję lub eskalację. Mapowanie do MITRE ATT&CK stosuje się, jeżeli charakter detekcji umożliwia wiarygodne przypisanie.

5. Reakcja i Threat Intelligence

Warstwa NDR musi umożliwiać przekazanie decyzji reakcyjnej do systemu zdolnego do egzekwowania polityki bezpieczeństwa. Dopuszcza się reakcję automatyczną lub półautomatyczną, w tym blokowanie adresów, domen/URL lub określonej komunikacji, wykonanie skryptu albo utworzenie incydentu.

Działania mogące wpływać na dostępność infrastruktury OT/ICS lub systemów krytycznych wymagają akceptacji uprawnionego operatora.

NDR musi wykorzystywać dostępne informacje Threat Intelligence, w tym co najmniej adresy IP, domeny, URL, hashe i informacje o malware, w zakresie obsługiwanym przez zintegrowane systemy.

6. Widoki analityczne i pokrycie

Wykonawca musi przygotować co najmniej jeden centralny widok NDR prezentujący istotne zdarzenia, w tym C2, IPS, malware, DNS, zdarzenia IT–OT, rekonesans, potencjalny lateral movement oraz trendy i najbardziej aktywne źródła.

Wykonawca musi określić poziom pokrycia monitorowanej infrastruktury oraz wskazać segmenty i klasy ruchu o widoczności pełnej, częściowej lub niewystarczającej. Dla istotnych luk należy wskazać rekomendowane działania poprawiające widoczność.

7. Możliwość rozbudowy

Architektura musi umożliwiać w przyszłości podłączenie niezależnego pasywnego sensora IDS/NDR poprzez SPAN, TAP, mirrorowanie ruchu lub mechanizm równoważny, bez konieczności wymiany wdrożonego UTM/NGFW i SIEM. Dostawa takiego sensora nie wchodzi w podstawowy zakres O14.

W ramach odbioru O14 Wykonawca wskaże komponenty realizujące funkcję NDR, źródła telemetrii, skonfigurowane klasy detekcji, zaprezentuje działanie wybranego przypadku detekcji oraz przekaże centralny widok i informację o pokryciu monitorowanej infrastruktury.

3.15.4. Licencjonowanie, gwarancja i dokumentacja Systemu SIEM

1. Wymagania licencyjne

1.1. Wykonawca zapewni Zamawiającemu bezterminową, niewyłączną licencję na korzystanie z Systemu SIEM, bez ograniczeń terytorialnych.

1.2. Licencja nie może wprowadzać ograniczeń dotyczących liczby przechowywanych danych ani liczby wykonywanych wyszukiwań.

1.3. Wykonawca zapewni możliwość aktualizowania Systemu do najnowszych wersji udostępnianych w ramach obowiązujących uprawnień licencyjnych i okresów wsparcia.

1.4. Zamawiający musi mieć możliwość zgłaszania błędów i nieprawidłowości bezpośrednio Wykonawcy.

1.5. Wymagania dotyczące licencji nie ograniczają możliwości zastosowania oprogramowania open source, pod warunkiem spełnienia wszystkich wymaganych funkcjonalności Systemu.

2. Gwarancja oprogramowania

2.1. Wykonawca zapewni gwarancję prawidłowego działania dostarczonego i wdrożonego Systemu SIEM na warunkach określonych w OPZ.

2.2. Gwarancja obejmuje w szczególności:

a) zapewnienie wersji oprogramowania wolnych od wad;

b) usuwanie usterek zdalnie lub na miejscu, stosownie do ich charakteru;
c) utrzymanie integralności baz danych;
d) dostarczanie aktualizacji wynikających ze zmian przepisów prawa lub rozwoju aplikacji, w zakresie objętym licencją i gwarancją;
e) informowanie Zamawiającego o krytycznych poprawkach bezpieczeństwa w terminie 7 dni od ich publicznego udostępnienia;
f) zapewnienie możliwości instalacji łat i poprawek bezpieczeństwa, jeżeli uprawnienia licencyjne umożliwiają ich pobranie i wykorzystanie.
2.3. Wymagania dotyczące gwarancji oprogramowania nie ograniczają obowiązków Wykonawcy w zakresie świadczenia usług wsparcia technicznego określonych w rozdziale 3.14.X OPZ.

3. Aktualizacje Systemu

3.1. System musi umożliwiać instalowanie aktualizacji oprogramowania, w tym aktualizacji bezpieczeństwa oraz poprawek eliminujących wykryte nieprawidłowości.
3.2. Wykonawca zapewni dostęp do aktualizacji na zasadach określonych w wymaganiach licencyjnych i gwarancyjnych.
3.3. Instalacja i konfiguracja aktualizacji w okresie świadczenia wsparcia technicznego realizowana będzie zgodnie z wymaganiami rozdziału 3.14.X OPZ.

4. Dokumentacja powykonawcza Systemu

4.1. Najpóźniej przy odbiorze końcowym Wykonawca przekaże Zamawiającemu kompletną dokumentację techniczną Systemu SIEM, obejmującą co najmniej:
a) wykaz zastosowanych bibliotek, modułów i funkcjonalności Systemu;
b) szczegółowy schemat bazy danych, w zakresie udostępnianym przez producenta lub wynikającym z zastosowanej architektury;
c) procedury aktualizacji Systemu;
d) procedury wykonywania i odtwarzania kopii zapasowych konfiguracji oraz danych Systemu;
e) wykaz zainstalowanych komponentów, ich wersji oraz zależności;
f) informacje o licencjach, okresach subskrypcji i przysługujących uprawnieniach;
g) pozostałe materiały niezbędne do prawidłowej administracji, eksploatacji i utrzymania Systemu.
4.2. Dokumentacja powykonawcza musi odpowiadać faktycznej konfiguracji wdrożonego Systemu SIEM.
4.3. W przypadku zastosowania komponentów, których producent nie udostępnia wewnętrznej struktury baz danych lub kodu źródłowego, Wykonawca przekaże dostępną dokumentację techniczną oraz opis interfejsów i mechanizmów umożliwiających eksploatację, aktualizację, wykonywanie kopii zapasowych i odtwarzanie Systemu.

3.16. Oprogramowanie MFA – O43 – 1 licencja

1. Dostawa Oprogramowania wraz z udzieleniem lub zapewnieniem udzielenia licencji przez Wykonawcę Systemu służącego do uwierzytelniania wieloskładnikowego użytkowników.
2. Oferowany System musi posiadać wsparcie techniczne w języku polskim.
3. Producentem Systemu musi być podmiot posiadający siedzibę w Unii Europejskiej.
4. W ramach przedmiotu zamówienia Wykonawca zobowiązuje się udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości, jak i poszczególnych jego elementów dla 40 użytkowników.

3.16.1. Oprogramowanie niezbędne do uruchomienia Systemu

I. Wymagania ogólne

1. System musi zawierać konsolę administracyjną dostępną z poziomu przeglądarki internetowej umożliwiającą administratorowi jego konfigurację oraz zarządzanie.
2. System musi umożliwiać samodzielną rejestrację uwierzytelniaczy (tokenów uwierzytelniających) przez użytkowników.
3. System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez zareagowanie na spersonalizowane powiadomienie wysyłane na urządzenie mobilne użytkownika.
4. System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez wpisanie kodu jednorazowego pochodzącego z dowolnej aplikacji generującej kody jednorazowe zgodnie ze standardem TOTP (RFC 6238). Przykładami takich aplikacji są Microsoft Authenticator oraz Google Authenticator.
5. System musi umożliwiać potwierdzenie żądania uwierzytelniania wieloskładnikowego poprzez wpisanie kodu jednorazowego wysłanego na numer telefonu użytkownika w postaci wiadomości SMS.
6. System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego poprzez kliknięcie w link wysłany na numer telefonu komórkowego użytkownika w postaci wiadomości SMS.
7. System musi umożliwiać zebranie zgody użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na numer telefonu użytkownika.
8. System musi umożliwiać wyświetlanie w konsoli administracyjnej informacji o udzielonej zgodzie od użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na wskazany numer telefonu.
9. System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego przy pomocy mobilnej aplikacji uwierzytelniającej, do której dostęp może być zabezpieczony przy pomocy blokady biometrycznej w postaci odcisku palca lub skanu twarzy, jeśli urządzenie mobilne użytkownika posiada taką techniczną możliwość.
10. System musi umożliwiać zakładanie kont administratorów mających dostęp do konsoli administracyjnej wraz z przypisaniem im roli stosownej do zakresu obowiązków danego administratora.
11. System musi umożliwiać identyfikowanie użytkowników po aliasach.
12. System musi umożliwiać udzielanie dostępu do określonych chronionych rozwiązań informatycznych tylko wybranym grupom użytkowników.
13. System musi wygaszać sesję administratora w konsoli administracyjnej w przypadku nieaktywności administratora.
14. System musi umożliwiać przeszukiwanie list zarejestrowanych przez użytkowników numerów telefonów oraz kluczy sprzętowych.

15. System musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia użytkowników w oparciu o zdefiniowane parametry, co najmniej takie jak: grupa, chroniony zasób oraz adres IP użytkownika.
16. System musi umożliwiać wygenerowanie tymczasowego kodu dostępowego dla wskazanego użytkownika w przypadku niedostępności uwierzytelniacza, np. zagubienia klucza uwierzytelniającego.
17. System musi zapewnić logowanie żądań uwierzytelniania użytkowników. System musi umożliwiać pobieranie logów w formacie CSV.
18. System musi zapewnić logowanie zdarzeń związanych z obsługą Systemu (wprowadzanie zmian w konfiguracji i politykach, logowanie działań administratorów). System musi umożliwiać pobieranie logów w formacie CSV.
19. System musi posiadać API (pol.: Interfejs Programowania Aplikacji) umożliwiające zarządzanie co najmniej użytkownikami.
20. System musi zapewnić interfejs użytkownika dokonującego uwierzytelniania do chronionych aplikacji w j. polskim.

II. Wymagane integracje

21. System musi zapewniać możliwość uruchomienia uwierzytelniania wieloskładnikowego dla rozwiązań uwierzytelniających użytkowników ze źródeł Active Directory (LDAP, LDAPS) i RADIUS.
22. System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows 7 i nowszymi wersjami oraz do serwerów z systemem operacyjnym Microsoft Windows Server 2008 R2 i nowszymi wersjami. W przypadku braku połączenia z Internetem musi być możliwe wykonanie uwierzytelnienia wieloskładnikowego przynajmniej w postaci jednorazowego hasła (One-Time Password, OTP).
23. System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla technologii: Microsoft Outlook Web App (OWA), Microsoft Remote Desktop Gateway/Web Access/Web Client/Web Feed oraz Microsoft Active Directory Federation Services (AD FS).
24. System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń przez protokół Remote Desktop Protocol (RDP).

System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego

3.17. Klucze sprzętowe U2F – S29

Dostarczyć 15 szt. kluczy sprzętowych USB/NFC, które służą do uwierzytelniania jedno-, dwu- i wieloskładnikowe. Urządzenie ma być zgodne z protokołami FIDO2/WebAuthn oraz U2F oraz OTP.

3.18. Zarządzalny przełącznik sieciowy IT i OT – S27 – 2 szt.

1. Porty przełącznika: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 6x 1/10GBase-X SFP+

a) Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ bez dedykowanego okablowania

Port konsolowy: RJ45 (RS-232)
Port zarządzania: RJ45 (10/100Base-T RJ45)
Port USB: minimum 1 port co najmniej w standardzie 2.0
Szybkość przełączania: minimum 168Gb/s
Przepustowość: minimum 125Mp/s (dla pakietów 64Kb)
Bufor pakietów: minimum 2MB
Ramki Jumbo: minimum 12k
Tablica adresów MAC: minimum 32k
Adresy MAC – Multicast: minimum 2k
Tablica ACL: minimum 3k
Tablica VLAN: minimum 4k
Tablica routingu: minimum 12k
Taktowanie procesora: minimum 1G
Pamięć Flash: minimum 32 MB + 128MB NAND
Pamięć RAM: minimum 1G
Temperatura pracy: zakres minimum 0°C - 50°C
Wilgotność względna: zakres minimum 5% - 90% (bez kondensacji)
Zasilanie: zasilacz modułowy 230V AC, możliwość instalacji drugiego zasilacza
Pobór mocy: maksymalnie 50W
Zabezpieczenie przeciwprzepięciowe: minimum 4kV
Wymiary: maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 380mm
Certyfikaty bezpieczeństwa: CE, RoHS

Algorytm pracy: Store and Forward
Obsługa VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ, Selective QinQ
DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
Drzewo rozpinające: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Root Guard, BPDU guard, BPDU forwarding,
Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms, Loopback Detection
Protokoły routingu: Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect, GRE Tunnel, ISIS
Agregacja linków: IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balance
Bezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, ND

Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast: IGMP v1/v2/v3 snooping, IGMP Query, IGMP multicast group, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, PIM-SM, PIM-DM, PIM-SSM, IGMP authentication
QoS: 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: SP, WRR, SP+WRR; WRED,
Lista Kontroli Dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Standard and Expanded ACL based on IP Protocol and IP Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route,
Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah OAM, ULDP (like UDLD), LLDP/LLDP MED, VSF (4 devices in one stack) – hardware stacking.
Przełączniki muszą obsługiwać MACsec zgodnie z IEEE 802.1AE. Wykonawca zapewni wszystkie licencje niezbędne do korzystania z tej funkcji oraz skonfiguruje ją na uzgodnionych połączeniach pomiędzy urządzeniami obsługującymi MACsec. Jeden przełącznik przeznaczony jest do obszaru IT, a drugi do obszaru OT. Dokumentacja powykonawcza wskaże ich lokalizację, rolę oraz sposób zapewnienia wymaganej redundancji połączeń.
Oprogramowanie oraz wsparcie techniczne: oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług.
Gwarancja: minimum 60 miesięcy

3.19. Router OT – O28

1. Przedmiot i zakres zamówienia

1.1. Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie jednego routera przeznaczonego do obsługi infrastruktury OT/ICS Zamawiającego.

1.2. Router będzie służył do zapewnienia bezpiecznej komunikacji pomiędzy wydzielonymi segmentami infrastruktury OT oraz systemami nadrzędnymi, z zachowaniem zasad segmentacji sieci i kontroli dostępu.

1.3. Urządzenie musi być przystosowane do pracy ciągłej 24/7 oraz zapewniać współpracę z infrastrukturą teleinformatyczną i przemysłową Zamawiającego.

2. Minimalne wymagania techniczne

2.1. Urządzenie musi posiadać co najmniej 4 interfejsy Ethernet RJ-45 10/100/1000 Mb/s.

2.2. Urządzenie musi obsługiwać routing statyczny IPv4.

2.3. Urządzenie musi obsługiwać sieci VLAN zgodnie ze standardem IEEE 802.1Q.

2.4. Urządzenie musi umożliwiać konfigurację reguł kontroli ruchu sieciowego (ACL lub firewall).

2.5. Urządzenie musi zapewniać obsługę szyfrowanych połączeń VPN IPsec.

2.6. Urządzenie musi obsługiwać protokoły DHCP oraz NTP.

2.7. Urządzenie musi umożliwiać zdalne zarządzanie przez szyfrowane połączenie HTTPS lub SSH.

2.8. Urządzenie musi umożliwiać rejestrowanie zdarzeń systemowych oraz przesyłanie logów do centralnego systemu monitorowania bezpieczeństwa, np. z wykorzystaniem protokołu Syslog.

2.9. Urządzenie musi umożliwiać wykonywanie kopii zapasowych konfiguracji oraz ich odtwarzanie.

2.10. Urządzenie musi zapewniać możliwość aktualizacji oprogramowania układowego (firmware).

3. Wymagania dotyczące bezpieczeństwa

3.1. Router musi umożliwiać logiczną separację infrastruktury OT od pozostałych segmentów sieci Zamawiającego.

3.2. Router musi umożliwiać ograniczenie komunikacji pomiędzy segmentami sieci zgodnie z zasadą minimalnych niezbędnych uprawnień.

3.3. Urządzenie musi zapewniać możliwość ograniczenia dostępu administracyjnego do określonych adresów IP lub podsieci.

3.4. Router musi współpracować z systemem UTM/NGFW dostarczonym w ramach zamówienia.

3.5. Konfiguracja urządzenia musi uwzględniać wymagania bezpieczeństwa infrastruktury OT/ICS, w szczególności ograniczenie dostępu zdalnego oraz zabezpieczenie komunikacji administracyjnej.

3.6. Wdrożenie routera nie może powodować zakłóceń pracy istniejących systemów sterowania i monitorowania procesów technologicznych.

4. Instalacja i konfiguracja

4.1. Wykonawca zobowiązany jest do dostarczenia i zainstalowania routera w lokalizacji wskazanej przez Zamawiającego.

4.2. Zakres prac obejmuje w szczególności:

a) konfigurację interfejsów sieciowych i adresacji IP;

b) konfigurację routingu i segmentacji sieci;

c) konfigurację reguł kontroli dostępu;

d) konfigurację bezpiecznej komunikacji z systemem UTM/NGFW;

e) konfigurację rejestrowania i przekazywania zdarzeń do systemu monitorowania;

f) zabezpieczenie dostępu administracyjnego;

g) wykonanie kopii zapasowej konfiguracji;

h) przeprowadzenie testów komunikacji i bezpieczeństwa.

4.3. Konfiguracja routera musi być zgodna z przyjętą architekturą sieci IT/OT Zamawiającego.

5. Gwarancja i wsparcie techniczne

5.1. Wymagany okres gwarancji na urządzenie wynosi minimum 36 miesięcy.

5.2. W okresie gwarancji Wykonawca zapewni dostęp do aktualizacji bezpieczeństwa oprogramowania układowego.

5.3. Wykonawca zapewni wszystkie licencje i subskrypcje niezbędne do działania wymaganych funkcjonalności przez okres minimum 36 miesięcy.

6. Dokumentacja i odbiór

6.1. Wykonawca przekaże Zamawiającemu dokumentację powdrożeniową obejmującą:

a) schemat podłączenia urządzenia do infrastruktury Zamawiającego;

b) opis konfiguracji interfejsów i routingu;

c) wykaz zastosowanych reguł bezpieczeństwa;

d) kopię konfiguracji urządzenia;

e) instrukcję wykonywania i odtwarzania kopii konfiguracji;

f) informacje dotyczące licencji i gwarancji.

6.2. Odbiór urządzenia obejmuje sprawdzenie:

a) prawidłowej komunikacji pomiędzy wymaganymi segmentami sieci;

b) skuteczności zastosowanych reguł kontroli dostępu;

c) współpracy z systemem UTM/NGFW;

d) przekazywania zdarzeń do systemu monitorowania;

e) poprawności wykonywania i odtwarzania konfiguracji.

6.3. Testy odbiorowe należy przeprowadzić w sposób niewpływający na ciągłość działania infrastruktury technologicznej Zamawiającego.

3.20. Usługi konfiguracji i hardeningu systemów oraz urządzeń IT/OT/ICS/IIoT – U39

1. Przedmiot i zakres usługi
1.1. Przedmiotem zamówienia jest wykonanie konfiguracji bezpieczeństwa oraz hardeningu systemów i urządzeń IT/OT/ICS/IIoT Zamawiającego objętych projektem.
1.2. Celem usługi jest ograniczenie powierzchni ataku, eliminacja zbędnych funkcjonalności i usług oraz podniesienie poziomu odporności infrastruktury na zagrożenia cyberbezpieczeństwa.
1.3. Zakres prac obejmuje, stosownie do rodzaju urządzeń i systemów:
a) serwery fizyczne i wirtualne;
b) systemy operacyjne;
c) urządzenia sieciowe;
d) urządzenia UTM/NGFW;
e) systemy zarządzania tożsamością i dostępem;
f) systemy kopii zapasowych;
g) stacje robocze objęte projektem;
h) systemy monitorowania i cyberbezpieczeństwa;
i) urządzenia i systemy OT/ICS/IIoT w zakresie uzgodnionym z Zamawiającym.
2. Wymagania dotyczące hardeningu systemów IT
2.1. Wykonawca przeprowadzi analizę aktualnej konfiguracji systemów i urządzeń objętych zakresem usługi.
2.2. Wykonawca zastosuje odpowiednie mechanizmy utwardzania konfiguracji, w szczególności:
a) wyłączenie zbędnych usług i protokołów;
b) wyłączenie lub zabezpieczenie nieużywanych interfejsów;
c) ograniczenie dostępu administracyjnego;
d) zmianę domyślnych danych uwierzytelniających;
e) wdrożenie zasad minimalnych uprawnień;
f) konfigurację mechanizmów kontroli dostępu;
g) konfigurację rejestrowania zdarzeń;
h) zabezpieczenie komunikacji administracyjnej;
i) konfigurację polityk bezpieczeństwa systemów operacyjnych;
j) weryfikację aktualności i ustawień mechanizmów bezpieczeństwa.

2.3. Wykonawca uwzględni zalecenia producentów oraz uznane dobre praktyki bezpieczeństwa, w szczególności CIS Benchmarks, jeżeli mają zastosowanie do danego systemu.
2.4. Wprowadzane zmiany muszą uwzględniać wymagania kompatybilności i dostępności systemów wykorzystywanych przez Zamawiającego.
3. Hardening infrastruktury sieciowej
3.1. Wykonawca przeprowadzi weryfikację i konfigurację zabezpieczeń urządzeń sieciowych objętych projektem.
3.2. Zakres prac obejmuje w szczególności:
a) weryfikację i ograniczenie dostępu administracyjnego;
b) konfigurację bezpiecznych protokołów zarządzania;
c) weryfikację reguł ACL i polityk firewall;
d) konfigurację segmentacji VLAN;
e) ograniczenie komunikacji pomiędzy wydzielonymi segmentami sieci;
f) wyłączenie nieużywanych portów i usług;
g) konfigurację rejestrowania zdarzeń;
h) zabezpieczenie dostępu zdalnego;
i) weryfikację konfiguracji urządzeń UTM/NGFW;
j) zabezpieczenie konfiguracji urządzeń przed nieautoryzowanymi zmianami.
4. Hardening infrastruktury OT/ICS/IIoT
4.1. Wykonawca przeprowadzi analizę konfiguracji bezpieczeństwa systemów i urządzeń OT objętych zakresem projektu.
4.2. Zakres prac może obejmować, stosownie do możliwości technicznych i zaleceń producentów:
a) ograniczenie dostępu administracyjnego;
b) zmianę domyślnych danych uwierzytelniających;
c) wyłączenie zbędnych usług komunikacyjnych;
d) konfigurację zasad komunikacji między strefami IT i OT;
e) ograniczenie zdalnego dostępu do urządzeń sterowania;
f) konfigurację rejestrowania zdarzeń;
g) zabezpieczenie interfejsów zarządzania;
h) wykonanie kopii konfiguracji urządzeń, jeżeli jest to technicznie możliwe.
4.3. Zmiany konfiguracji urządzeń PLC, HMI, SCADA oraz innych urządzeń przemysłowych mogą być wykonywane wyłącznie po uzgodnieniu z Zamawiającym oraz po potwierdzeniu ich bezpieczeństwa dla procesów technologicznych.
4.4. Nie dopuszcza się wprowadzania zmian mogących powodować niekontrolowane zatrzymanie urządzeń lub zakłócenie ciągłości pracy infrastruktury technologicznej.
4.5. W przypadku braku możliwości bezpiecznego wdrożenia określonych zabezpieczeń Wykonawca wskaże ograniczenia oraz zaproponuje alternatywne środki ograniczenia ryzyka.
5. Konfiguracja systemów bezpieczeństwa
5.1. Wykonawca zapewni właściwą konfigurację mechanizmów bezpieczeństwa w ramach dostarczonych i wdrożonych rozwiązań.
5.2. Zakres obejmuje w szczególności:
a) konfigurację zasad uwierzytelniania i autoryzacji;
b) konfigurację polityk dostępu;
c) konfigurację mechanizmów rejestrowania zdarzeń;
d) integrację wymaganych źródeł zdarzeń z systemem SIEM;

e) konfigurację mechanizmów zabezpieczających dostęp administracyjny;
f) weryfikację poprawności działania wdrożonych zabezpieczeń.
5.3. Czynności konfiguracji i hardeningu muszą być spójne z pozostałymi rozwiązaniami dostarczonymi w ramach zamówienia.
6. Dokumentacja powdrożeniowa
6.1. Wykonawca opracuje dokumentację wykonanych prac obejmującą:
a) wykaz systemów i urządzeń objętych hardeningiem;
b) opis stanu konfiguracji przed wykonaniem prac;
c) wykaz wprowadzonych zmian;
d) opis zastosowanych mechanizmów bezpieczeństwa;
e) wykaz odstępstw od zalecanych konfiguracji wraz z uzasadnieniem;
f) opis ograniczeń i ryzyk pozostających po wdrożeniu zabezpieczeń;
g) procedury odtworzenia konfiguracji, w zakresie technicznie możliwym.
6.2. Wykonawca przekaże Zamawiającemu kopie konfiguracji urządzeń i systemów w zakresie wynikającym z możliwości technicznych i uprawnień licencyjnych.
7. Testy i odbiór
7.1. Po wykonaniu prac Wykonawca przeprowadzi kontrolę poprawności zastosowanych konfiguracji.
7.2. Testy obejmą w szczególności:
a) weryfikację dostępu administracyjnego;
b) sprawdzenie działania mechanizmów uwierzytelniania;
c) weryfikację ograniczeń komunikacji sieciowej;
d) sprawdzenie rejestrowania zdarzeń;
e) potwierdzenie dostępności kluczowych usług i systemów;
f) sprawdzenie, czy wprowadzone zmiany nie zakłóciły funkcjonowania infrastruktury.
7.3. Odbiór usługi nastąpi na podstawie dokumentacji wykonanych prac oraz potwierdzenia poprawności konfiguracji i działania zabezpieczeń.
7.4. W przypadku infrastruktury OT testy odbiorowe muszą być prowadzone w sposób zapewniający bezpieczeństwo procesów technologicznych.

3.21. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS

3.21.1. Przedmiot i cel szkolenia

Przedmiotem zamówienia jest przygotowanie i przeprowadzenie szkolenia administratorów IT oraz pracowników odpowiedzialnych za eksploatację i bezpieczeństwo systemów OT/ICS Zakład Usług Gminnych Gmina Ełk Sp. z o.o. Szkolenie stanowi realizację zadania 2, pozycja 2.1.3, kategoria U28.

Celem jest przygotowanie uczestników do bezpiecznej eksploatacji, bieżącego nadzoru i podstawowej

administracji środkami bezpieczeństwa zastosowanymi lub planowanymi do zastosowania w zadaniach 3 i 4 projektu, rozpoznawania zdarzeń wymagających reakcji oraz postępowania zgodnie z procedurami Zamawiającego. Program musi odnosić się do faktycznie wdrożonej architektury, wersji systemów i konfiguracji.

3.21.2. Uczestnicy czas i forma

Szkolenie obejmie jedną grupę liczącą do 3 osób wskazanych przez Zamawiającego. Zajęcia odbędą się w języku polskim, stacjonarnie w siedzibie Zamawiającego; część zdalna jest dopuszczalna za uzgodnieniem, jeżeli zapewnia równoważny udział w ćwiczeniach.

3.21.3. Minimalny program szkolenia

1. Architektura i bezpieczeństwo IT OT

Strefy IT/OT i DMZ, role UTM/NGFW, switchy i Wi-Fi, dozwolone przepływy, VLAN, dostęp zdalny i zasady zmian. Rola administratorów, operatorów oraz dostawców; wpływ reakcji bezpieczeństwa na ciągłość dostaw wody i procesy oczyszczania.

2. Sieć i kontrolowany dostęp

Obsługa wdrożonych UTM/NGFW, przegląd reguł, VPN, IPS/IDS i dostępnych mechanizmów ochrony WWW/DNS/sandbox. Uwierzytelnianie Wi-Fi i RADIUS, przegląd konfiguracji switchy i diagnostyka połączeń. Zarządzanie uprawnieniami w AD, MFA i kluczami FIDO2/U2F, menedżerem haseł oraz PAM/JIT i PAW/stacją przesiadkową zgodnie z przyjętą architekturą.

3. Ochrona endpointów danych i poczty

Konsola AV/EDR, polityki ochrony ransomware, sprawdzanie stanu ochrony i aktualizacji, UEM, inwentaryzacja, DLP i zdarzenia naruszeń. Ochrona poczty, kwarantanna, phishing/BEC i zgłaszanie podejrzanych wiadomości. Podstawowa obsługa WAF oraz nadzór nad ważnością certyfikatów TLS.

4. Monitoring i analiza zdarzeń

SIEM, menedżer logów, dashboardy, wyszukiwanie i interpretacja alertów; relacje XDR, ITDR i NDR do źródeł danych. Priorytetyzacja zdarzeń i podatności, false positive, utrata telemetrii, współpraca z MIDS/MDR/CTI zgodnie z zakupionymi usługami. Monitoring infrastruktury i sensorów OT objętych wdrożeniem.

3.21.4. Program praktyczny i zasady odbioru szkolenia

1. Serwery kopie zapasowe i ciągłość

Nadzór nad serwerami, systemami operacyjnymi, wirtualizacją, zasobami NAS i HA. Harmonogramy, retencja, szyfrowanie i niezmienność kopii, sprawdzanie wyniku backupu, odtwarzanie pliku i testowej maszyny, kopie konfiguracji oraz uzgodnione RPO/RTO. Obsługa alarmów UPS, kolejność bezpiecznego wyłączenia i uruchomienia usług. Platforma kontenerowa w zakresie objętym wdrożeniem.

2. Eksploatacja OT i obsługa incydentu

Bezpieczny monitoring PLC/HMI/SCADA i komunikacji przemysłowej, analiza alertów sensorów i IPS OT, ograniczenia skanowania i aktualizacji. Dostęp serwisowy dostawcy, zasady zatwierdzania zmian, dokumentacja aktywów oraz zgłoszenia i zmiany w ITSM. Analiza incydentu, zabezpieczenie dowodów, eskalacja i odtwarzanie. PKI w zakresie rzeczywiście wdrożonym.

3.21.5. Materiały dokumentowanie i odbiór

Wykonawca przekaże w języku polskim program z czasem modułów, materiały PDF, instrukcje wykonania ćwiczeń, krótkie instrukcje eksploatacyjne wdrożonych rozwiązań oraz ścieżkę zgłaszania awarii i incydentów. Dokumentacja wykonania obejmie listę obecności lub równoważne potwierdzenie udziału, daty i czas zajęć, dane prowadzącego, protokół z wykonanych ćwiczeń, wyniki krótkiej weryfikacji wiedzy i zaświadczenia uczestnictwa.

Warunkiem odbioru jest wykonanie programu i ćwiczeń, dotrzymanie wymiaru zajęć oraz przekazanie dokumentacji. Wykonawca omówi błędy ujawnione podczas ćwiczeń lub weryfikacji wiedzy. Cena szkolenia obejmuje przygotowanie, prowadzenie, dojazd, środowisko ćwiczeniowe, materiały i dokumentację. Zakres i wynagrodzenie U28 należy wykazać odrębnie od instruktażu dostawcy oraz szkoleń U26, U27 i U29, bez ponownego rozliczania tych samych czynności.