

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

Część 1 - Obszar organizacyjny i Audyt	4
Zadanie 1. Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z dokumentacją Systemu Zarządzania Ciągłością Działania (SZCD)	4
Zadanie 2. Audyt SZBI i SZCD, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów. 8	
Zadanie 3. Audyt cyberbezpieczeństwa sieci IT/OT/ICS/IloT	10
Część 2 - Obszar kompetencyjny oraz obszar techniczny IT/OT	12
Zadanie 1. Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyber-zagrożeń i sposobów ochrony dla pracowników IT/OT/ICS.	12
Zadanie 2. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS	15
Zadanie 3. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS	16
Zadanie 4. Wykonanie szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami IT/OT/ICS	17
Zadanie 5. Usługi typu security awareness do symulowanych ataków socjotechnicznych IT/OT/ICS dostępu do portalu dla pracowników Zamawiającego	19
Zadanie 6. Oprogramowanie do badania podatności	21
Zadanie 7. Oprogramowanie do ochrony przed ransomware	24
Zadanie 8. Oprogramowanie typu EDR (Endpoint Detection and Response)	29
Zadanie 9. Urządzenie i oprogramowanie typu NDR z HoneyPot i monitorem sytuacyjnym (Network Detection & Response)	34
Zadanie 10. Zaprojektowanie i wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT. Profesjonalna usługa wdrożenia rozwiązań	39
Zadanie 11. System typu NGFW dla sieci IT HA	40
Zadanie 12. System typu NGFW dla sieci IT HA	46
Zadanie 13. Usługi konfiguracji i hardeningu systemów/urządzeń IT	51

Zadanie 14.	Stacja robocza fizyczna z rolą stacji przesiadkowej + dwa monitory 27 cali	51
Zadanie 15.	Usługa segmentacji sieci.....	53
Zadanie 16.	Serwer do wykonywania kopii zapasowych (NAS)	54
Zadanie 17.	System operacyjny na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa	62
Zadanie 18.	Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa pod system wirtualizacji (SIEM OT)	63
Zadanie 19.	Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa pod rozwiązania bezpieczeństwa	65
Zadanie 20.	Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa.....	67
Zadanie 21.	Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X/68	
Zadanie 22.	Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise	69
Zadanie 23.	Oprogramowanie typu ITSM (Information Technology Service Management)	70
Zadanie 24.	Oprogramowanie typu MDM (Mobile Device Management)	72
Zadanie 25.	Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention) 75	
Zadanie 26.	Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT	78
Zadanie 27.	Oprogramowanie do zarządzania tożsamością i dostępem w trybie brokera sesji 80	
Zadanie 28.	Oprogramowanie lub urządzenie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie)	81
Zadanie 29.	Klucze sprzętowe U2F	82
Zadanie 30.	Usługa inwentaryzacji aktywów teleinformatycznych IT.....	83
Zadanie 31.	Dostawa sprzętowych sondy/sensory do monitorowania sieci OT – montaż RACK 19" (dedykowane urządzenia do analizy protokołów przemysłowych)	86
Zadanie 32.	Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych)	92
Zadanie 33.	Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT. Oprogramowanie platformowe, zintegrowany System bezpieczeństwa IPS/IDS, OT Anomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat), SIEM, AKPIA RSDT, XDR, NDR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT	98
Zadanie 34.	UTM (Unified Threat Management) Platforma sprzętowa DIN35 - System bezpieczeństwa IPS/IDS, OT Anomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat) , AI Sanitization, AI MGMT, ZBFW .	112

Zadanie 35.	Usługa Private APN	118
Zadanie 36.	Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa	121
Zadanie 37.	Usługa inwentaryzacji aktywów teleinformatycznych OT.	123
Zadanie 38.	Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doбором urządzeń, oprogramowania i usług wdrożenia i eksploatacji OT/ICS/IIoT	126
Zadanie 39.	Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source OT/ICS/IIoT	129
Zadanie 40.	Testy bezpieczeństwa infrastruktury sieciowej OT/ICS/IIoT	131
Zadanie 41.	Usługi konfiguracji i hardeningu systemów/urządzeń OT	136
Postanowienia końcowe i wymagania wobec dostaw i Wykonawcy dla części 2		137



Część 1 - Obszar organizacyjny i Audyt

Zadanie 1. Opracowanie, wdrożenie, przegląd, aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z dokumentacją Systemu Zarządzania Ciągłości Działania (SZCD)

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest opracowanie, wdrożenie, przegląd oraz aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Systemu Zarządzania Ciągłości Działania (SZCD) u Zamawiającego – przedsiębiorstwa wodociągowo-kanalizacyjnego - zgodnie z wymaganiami:

- normy PN-EN ISO/IEC 27001 (aktualna wersja obowiązująca w dniu realizacji zadania),
- norm PN-EN ISO 22301 oraz powiązanych norm z rodziny 223xx dotyczących systemów zarządzania ciągłością działania,
- przepisów Ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm., wraz z nowelizacjami),
- innych obowiązujących przepisów prawa dotyczących ochrony informacji, w tym ochrony danych osobowych oraz zapewnienia odporności i ciągłości działania usług kluczowych.

1.2. Systemy SZBI i SZCD powinny zostać przygotowane w sposób umożliwiający:

- przeprowadzenie audytu zgodności z normą ISO/IEC 27001 oraz wymaganiami KSC,
- przeprowadzenie audytu zgodności z normą ISO 22301 oraz wymaganiami dotyczącymi ciągłości działania usług świadczonych przez przedsiębiorstwo wodociągowo-kanalizacyjne,
- zapewnienie spójności między SZBI i SZCD, ze szczególnym uwzględnieniem analizy ryzyka, analizy wpływu na biznes (BIA), planów ciągłości działania (BCP), planów odtwarzania (DRP) oraz procedur reagowania na incydenty.

2. Cel realizacji zamówienia

2.1. Celem realizacji zadania jest:

- Utworzenie lub aktualizacja kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z ISO/IEC 27001.
- Utworzenie lub aktualizacja Systemu Zarządzania Ciągłości Działania (SZCD) zgodnego z ISO 22301, obejmującego m.in. analizę BIA, strategię ciągłości działania, plany BCP/DRP oraz mechanizmy testowania i doskonalenia.
- Zapewnienie zgodności organizacji z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, w szczególności w zakresie obowiązków dotyczących organizacyjnych i technicznych środków bezpieczeństwa, raportowania incydentów oraz odporności i ciągłości działania.
- Zapewnienie spójności SZBI i SZCD z wymaganiami przyszłego audytu, obejmującego audyt zgodności z ISO/IEC 27001, ISO 22301 oraz wymaganiami KSC.

- Podniesienie poziomu bezpieczeństwa informacji oraz odporności operacyjnej organizacji poprzez wdrożenie właściwych zabezpieczeń organizacyjnych, proceduralnych i technicznych.
- Zapewnienie systemowego, opartego na ryzyku podejścia do zarządzania bezpieczeństwem informacji, ciągłości działania oraz cyberbezpieczeństwem.

3. Zakres prac

3.1. Zakres prac obejmuje opracowanie, wdrożenie oraz przegląd **SZBI oraz SZCD** w następujących obszarach:

- W ramach realizacji zamówienia Wykonawca opracuje lub zaktualizuje elementy organizacyjne **SZBI i SZCD**, obejmujące w szczególności:
 - **Strukturę organizacyjną bezpieczeństwa informacji i ciągłości działania**, w tym:
 - określenie ról i odpowiedzialności
 - wyznaczenie właścicieli procesów bezpieczeństwa i ciągłości działania,
 - określenie zasad eskalacji w sytuacjach kryzysowych.
 - **Politykę bezpieczeństwa informacji oraz Politykę ciągłości działania**, zapewniające spójność pomiędzy SZBI i SZCD.
 - **Zestaw procedur, instrukcji i regulacji SZBI i SZCD**, w szczególności dotyczących:
 - zarządzania bezpieczeństwem informacji,
 - zarządzania ciągłością działania,
 - zarządzania dostępem do informacji,
 - zarządzania incydentami (w tym incydentami poważnymi zgodnie z KSC),
 - zarządzania zmianą,
 - zarządzania kopiami zapasowymi i odtwarzaniem środowisk,
 - zarządzania dostawcami i usługami krytycznymi,
 - utrzymania i testowania planów ciągłości działania (BCP/DRP).
 - **System nadzoru nad dokumentacją SZBI i SZCD**, obejmujący:
 - sposób tworzenia,
 - zatwierdzania,
 - aktualizacji,
 - archiwizacji dokumentacji,
 - wersjonowanie dokumentów systemowych.
 - **Proces zarządzania ryzykiem bezpieczeństwa informacji i ryzykiem ciągłości działania**, zgodny z ISO/IEC 27005 oraz ISO 22301, obejmujący m.in. integrację wyników analiz ryzyka dla SZBI i SZCD.

3.2. Zakres prawny i formalny

- Wykonawca zapewni zgodność SZBI i SZCD z obowiązującymi przepisami prawa, w szczególności:
 - ustawą o Krajowym Systemie Cyberbezpieczeństwa,
 - przepisami dotyczącymi ochrony danych osobowych,
 - regulacjami dotyczącymi sektora istotnego i wymagań dotyczących odporności i ciągłości działania usług,
 - normami ISO/IEC 27001 oraz ISO 22301.

3.3. Zarządzanie ryzykiem

- Wykonawca zobowiązany jest do:
 - przeprowadzenia lub aktualizacji analizy ryzyka bezpieczeństwa informacji,
 - przeprowadzenia lub aktualizacji analizy wpływu na ciągłość działania (BIA),
 - opracowania spójnej metodyki zarządzania ryzykiem dla SZBI i SZCD,
 - identyfikacji aktywów informacyjnych i procesów krytycznych,
 - identyfikacji zagrożeń i podatności,
 - określenia poziomu ryzyka,
 - opracowania planu postępowania z ryzykiem,
 - powiązania poziomów ryzyka z wymaganymi planami ciągłości działania.

3.4. Deklaracja Stosowania (SoA)

- W ramach realizacji zadania Wykonawca opracuje lub zaktualizuje:
 - Deklarację Stosowania (Statement of Applicability – SoA) zgodną z ISO/IEC 27001,
 - powiązanie SoA z wymaganiami ciągłości działania (ISO 22301),
 - wykaz stosowanych zabezpieczeń wraz z uzasadnieniem,
 - wykaz zabezpieczeń wyłączonych wraz z uzasadnieniem.

3.5. Wdrożenie SZBI i SZCD

- W ramach wdrożenia Wykonawca zobowiązany jest do:
 - przeprowadzenia warsztatów wdrożeniowych dotyczących SZBI i SZCD,
 - przeszkolenia personelu odpowiedzialnego za bezpieczeństwo informacji i ciągłość działania,
 - przygotowania organizacji do testów planów ciągłości działania (BCP/DRP).

3.6. Przegląd i aktualizacja SZBI i SZCD

- Po wdrożeniu Wykonawca przeprowadzi:
 - weryfikację zgodności z wymaganiami norm ISO/IEC 27001 oraz ISO 22301,
 - weryfikację zgodności z przepisami KSC,
 - aktualizację dokumentacji systemowej,
 - rekomendacje działań usprawniających.

- Celem przeglądu jest zapewnienie gotowości organizacji do przeprowadzenia audytu SZBI i SZCD zgodnie z zakresem określonym przez Zamawiającego.

4. Produkty końcowe - Wykonawca zobowiązany jest do przekazania:

4.1. Kompletniej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania, obejmującej m.in.:

- Dokumentacja SZBI:
 - Politykę Bezpieczeństwa Informacji,
 - zestaw procedur i instrukcji SZBI,
 - metodykę zarządzania ryzykiem bezpieczeństwa informacji,
 - raport z analizy ryzyka,
 - plan postępowania z ryzykiem,
 - Deklarację Stosowania (SoA).
- Dokumentacja SZCD:
 - Politykę Ciągłości Działania,
 - analizę wpływu na ciągłość działania (BIA),
 - analizę ryzyka dla procesów krytycznych,
 - strategię ciągłości działania,
 - plany ciągłości działania (BCP),
 - plany odtwarzania po awarii (DRP),
 - procedury uruchamiania, testowania i utrzymania planów BCP/DRP,
 - harmonogram i metodykę testów ciągłości działania.

4.2. Raportu z wdrożenia **SZBI i SZCD**

- Raport powinien obejmować:
 - opis wykonanych prac,
 - listę zidentyfikowanych luk oraz rekomendacje działań doskonalących,
 - wyniki testów ciągłości działania (jeśli przewidziane w harmonogramie).

4.3. Materiałów szkoleniowych

- Wykonawca prześle szkolenia dla personelu odpowiedzialnego za SZBI i SZCD w postaci szkoleń e-Learning w paczkach SCORM oraz w postaci interaktywnych prezentacji. Należy przez to rozumieć, że paczka SCORM musi być możliwa do implementacji na platformie e-Learning Moodle.

4.4. Dokumentacji w formie:

- elektronicznej (DOCX, CHM oraz PDF),
- kompletnej, uporządkowanej strukturalnie, umożliwiającej bezpośrednie użycie podczas audytów i przeglądów systemowych.

Zadanie 2. Audyt SZBI i SZCD, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów.

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest przeprowadzenie kompleksowego audytu:

- Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- Systemu Zarządzania Ciągłością Działania (SZCD)

funkcjonujących u Zamawiającego – przedsiębiorstwa wodociągowo-kanalizacyjnego – w odniesieniu do wymagań norm:

- PN-EN ISO/IEC 27001 (aktualna wersja obowiązująca w dniu realizacji audytu)
- PN-EN ISO 22301 (aktualna wersja obowiązująca w dniu realizacji audytu)
- oraz wymagań nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa Dz.U. 2018 poz. 1560 zgodnie z informacją z dnia 23 stycznia 2026 r.

1.2. Dokument raportu z audytu winien pokrywać zakres opisany w szablonie audytu dla operatorów usług kluczowych dostępnym pod adresem:

<https://www.gov.pl/web/baza-wiedzy/szablony-audyty-dla-operatorow-uslug-kluczowych>

2. Cel realizacji zamówienia

2.1. Audyt ma na celu:

- Ocenę zgodności SZBI z wymaganiami normy PN-EN ISO/IEC 27001.
- Ocenę zgodności SZCD z wymaganiami normy PN-EN ISO/IEC 22301.
- Ocenę skuteczności wdrożonych zabezpieczeń organizacyjnych i technicznych oraz mechanizmów zapewnienia ciągłości działania.
- Identyfikację niezgodności, podatności oraz obszarów do doskonalenia.
- Weryfikację adekwatności analizy ryzyka oraz planów postępowania z ryzykiem i ciągłością działania.
- Ocenę zdolności organizacji do utrzymania ciągłości świadczenia usług w sytuacjach zakłóceń, incydentów lub awarii.
- Z wyłączeniem oceny zgodności z przepisami prawa w zakresie ochrony informacji niejawnych

3. Zakres prac

3.1. Audyt powinien obejmować co najmniej:

- Zakres organizacyjny:
 - strukturę organizacyjną w zakresie bezpieczeństwa informacji i ciągłości działania,
 - role i odpowiedzialności (w tym zespoły kryzysowe),
 - polityki, procedury i instrukcje SZBI oraz SZCD,
 - zarządzanie ryzykiem oraz analizę wpływu na działalność (BIA),
 - zarządzanie ryzykiem,
 - nadzór nad dokumentacją,
 - zarządzanie ciągłością działania i planami odtworzeniowymi.
- Zakres techniczny:
 - zabezpieczenia infrastruktury IT i OT (jeżeli objęte zakresem SZBI/SZCD),
 - kontrolę dostępu,
 - zarządzanie tożsamością,
 - zabezpieczenia sieciowe,
 - systemy kopii zapasowych i odtwarzania danych,
 - mechanizmy zapewnienia wysokiej dostępności,
 - monitoring bezpieczeństwa i ciągłości działania,
 - zarządzanie incydentami oraz zdarzeniami zakłócającymi ciągłość działania.
- Zakres prawny i formalny:
 - zgodność z przepisami dotyczącymi ochrony danych osobowych,
 - zgodność z wymaganiami dotyczącymi ciągłości działania wynikającymi z KRI i uoKSC
- Weryfikację:
 - analizy ryzyka,
 - Deklaracji Stosowania (SoA),
 - dokumentacji SZCD (BIA, BCP, DRP),
 - skuteczności działań korygujących z poprzednich audytów (jeżeli były realizowane),
 - wyników testów planów ciągłości działania.
- Zakres ciągłości działania
 - analizę wpływu na działalność (BIA – Business Impact Analysis),
identyfikację procesów krytycznych,
określenie parametrów:
 - RTO (Recovery Time Objective),
 - RPO (Recovery Point Objective),
 - ocenę planów ciągłości działania (BCP – Business Continuity Plan),
 - ocenę planów odtworzeniowych (DRP – Disaster Recovery Plan),
 - weryfikację procedur reagowania kryzysowego,
 - ocenę gotowości organizacji do działania w sytuacjach awaryjnych,
 - ocenę mechanizmów zapewnienia ciągłości usług dla infrastruktury krytycznej,
 - analizę redundancji systemów i zasobów (IT/OT),
 - ocenę zarządzania dostawcami w kontekście ciągłości działania.

3.2. Metodyka realizacji

- Audyt powinien zostać przeprowadzony zgodnie z:

- wytycznymi ISO 19011 (Wytyczne dotyczące auditowania systemów zarządzania),
 - zasadami bezstronności i niezależności audytorskiej,
 - zasadą poufności informacji.
- Audyt powinien obejmować:
 - przegląd dokumentacji,
 - wywiady z pracownikami,
 - wizję lokalną,
 - przegląd zabezpieczeń technicznych,
 - analizę próbek dowodów.

4. Produkty końcowe

4.1. Wykonawca zobowiązany jest do przekazania:

- Raportu z audytu zawierającego:
 - opis zakresu audytu,
 - zastosowaną metodykę,
 - wykaz stwierdzonych niezgodności (podział na: duże i małe),
 - spostrzeżenia i rekomendacje,
- ocenę dojrzałości SZBI,
- podsumowanie dla kierownictwa (Executive Summary).
- ocenę dojrzałości SZCD,
- ocenę zdolności organizacji do zapewnienia ciągłości działania,
- identyfikację ryzyk związanych z przerwaniem działania,
- rekomendacje w zakresie:
 - poprawy odporności organizacyjnej,
 - zwiększenia dostępności systemów IT/OT,
 - usprawnienia planów ciągłości działania i odtwarzania.
- Listy rekomendowanych działań korygujących.
- Raport powinien zostać przekazany w formie:
 - elektronicznej (PDF) podpisanej podpisem kwalifikowanym przez audytorów wiodących,

Zadanie 3. Audyt cyberbezpieczeństwa sieci IT/OT/ICS/IIoT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie niezależnego audytu bezpieczeństwa systemów IT oraz wdrożonych zabezpieczeń (technicznych i organizacyjnych). Celem audytu jest weryfikacja poprawności konfiguracji, skuteczności działania nowych rozwiązań oraz ich zgodności z dokumentacją projektową i normami (np. ISO/IEC 27001, wytyczne NIST lub KSC).

2. Zakres prac audytowych

- 2.1. Wykonawca przeprowadzi audyt w następujących obszarach:
Weryfikacja konfiguracji (Configuration Audit):

- Sprawdzenie poprawności wdrożenia urządzeń (Firewall, IPS/IDS, NDR, honeypot).
- Weryfikacja bezpiecznej konfiguracji systemów operacyjnych i baz danych (Hardening).
- Testy penetracyjne i podatności:
 - Wykonanie skanowania podatności wewnątrz nowo wydzielonych segmentów sieci.
 - Próba obejścia wdrożonych zabezpieczeń (testy WiFi, próby nieautoryzowanego dostępu do serwerów).
 - Weryfikacja poprawności działania mechanizmów wieloskładnikowego uwierzytelniania (MFA).
- Kontrola uprawnień administracyjnych i mechanizmów logowania.
- Weryfikacja ciągłości działania i kopii zapasowych:
- Sprawdzenie odporności systemów na awarie (testy High Availability/Failover).

3. Metodyka przeprowadzenia audytu

- 3.1. Metoda: Wykonawca przeprowadzi testy z pełną wiedzą o systemie, symulując realny atak.
- 3.2. Wywiady: Rozmowy z administratorami oraz analiza procedur operacyjnych stworzonych po wdrożeniu
- 3.3. Zgodność (Compliance): Sprawdzenie czy wdrożenie spełnia wymogi prawne (RODO, Ustawa o Krajowym Systemie Cyberbezpieczeństwa).

4. Produkty końcowe (Dostarczane przez Wykonawcę)

- 5.1. Raport z audytu:
 - Szczegółowy opis zidentyfikowanych podatności i błędów w konfiguracji
- 5.2. Karta zaleceń (Remediation Plan):
 - Lista konkretnych kroków naprawczych uszeregowanych według priorytetu (krytyczne, wysokie, średnie, niskie).

Wymagania dla wykonawcy części I:

4.2. Wykonawca musi:

- posiadać doświadczenie w realizacji co najmniej 5 audytów Systemu Zarządzania Bezpieczeństwem Informacji zgodnych z ISO/IEC 27001 w ciągu ostatnich 3 lat poparte referencjami, protokołami odbioru albo innymi dokumentami potwierdzającymi realizację zadania,
- posiadać certyfikat potwierdzający wdrożenie i stosowanie normy ISO 27001 wydany przez organizację akredytowaną przez Polskie Centrum Akredytacji (PCA). Wymóg certyfikatu ISO 27001 zapewnia, że Wykonawca posiada potwierdzoną dojrzałość w obszarze bezpieczeństwa informacji, co jest niezbędne do rzetelnego wykonania audytu i spełnienia obowiązków wynikających z nowej ustawy o KSC; wymóg dotyczy wyłącznie Wykonawcy,
- posiadać certyfikat potwierdzający wdrożenie i stosowanie normy ISO 22301 wydany przez organizację akredytowaną przez Polskie Centrum Akredytacji (PCA). Wymóg certyfikatu ISO 22301 gwarantuje, że Wykonawca posiada zweryfikowaną zdolność ciągłości

działania, co minimalizuje ryzyka realizacyjne audytu w środowisku podmiotu ważnego/kluczowego zgodnie z ustawą o KSC; wymóg odnosi się jedynie do Wykonawcy,

- zapewnić niezależność od Zamawiającego (brak konfliktu interesów),
- zapewnić poufność informacji uzyskanych w trakcie realizacji audytu,

4.3. Wymagania wobec personelu audytowego

W celu zachowania ciągłości audytu, musi on być prowadzony przez co najmniej dwóch audytorów. Zespół musi spełniać łącznie następujące wymagania:

- Posiadanie ważnego certyfikatu ISO/IEC 27001, wydanego przez jednostkę certyfikującą akredytowaną przez Polskie Centrum Akredytacji (PCA) (co najmniej dwie osoby).
- Udokumentowane doświadczenie w przeprowadzeniu minimum 5 audytów bezpieczeństwa w oparciu o normę ISO/IEC 27001 jako audytor wiodący (co najmniej dwie osoby).
- Znajomość przepisów:
 - ustawy o ochronie informacji niejawnych,
 - ustawy o krajowym systemie cyberbezpieczeństwa (jeżeli dotyczy),
 - przepisów dotyczących infrastruktury krytycznej.
- Poufność i bezpieczeństwo informacji
 - Wykonawca zobowiązany jest do podpisania umowy o zachowaniu poufności,
 - Dokumentacja audytowa nie może być przechowywana poza terytorium Europejskiego Obszaru Gospodarczego bez zgody Zamawiającego. Dokumentacja musi być przechowywana w formie zaszyfrowanej algorytmem minimum AES-256 albo lepszym.
 - Przekazywanie dokumentów musi odbywać się z wykorzystaniem bezpiecznych kanałów komunikacji przez co należy rozumieć, że cała komunikacja ma być szyfrowana.

Część 2 - Obszar kompetencyjny oraz obszar techniczny IT/OT

Zadanie 1. Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyber-zagrożeń i sposobów ochrony dla pracowników IT/OT/ICS.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest realizacja podstawowego szkolenia dla 2 osób z zakresu świadomości cyberzagrożeń poprzez usługę dostępu do platformy szkoleniowej dla pracowników „Kompleksowa Usługa Podnoszenia Świadomości Bezpieczeństwa”, umożliwiającą przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w Internecie, bezpieczeństwa informacji podczas pracy zdalnej oraz bezpieczeństwa IT przy codziennych obowiązkach.

1.1. Wykonawca musi dostarczyć platformę dedykowaną użytkownikom Zamawiającego, świadczoną przez okres min. do 30.06.2026.

- 1.2. Platforma musi być dostępna za pomocą dowolnej, nowoczesnej przeglądarki internetowej (Chrome, Firefox, Edge) a sama usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej.
- 1.3. Dostęp dla użytkownika musi odbywać się minimum w języku polskim, angielskim oraz trzecim wybranym przez Zamawiającego języku
- 1.4. Podczas tworzenia użytkownika, musi być możliwość wyboru domyślnego języka, w którym będzie on otrzymywał powiadomienia oraz w którym będzie miał dostęp do szkoleń. Niedopuszczalnym jest konieczność tworzenia osobnego kursu per każdy z dostępnych dla Zamawiającego języków.

2. Wymagania dotyczące platformy:

Usługa musi zawierać poszczególne komponenty:

2.1. Platforma szkoleniowa:

- Platforma musi zawierać minimum 280 szkoleń, dostępnych w języku polskim. Wszystkie szkolenia dostępne w języku polskim muszą być również dostępne w języku angielskim.
- W przypadku trzeciego języka liczba szkoleń może być mniejsza, natomiast wymaga się nie mniej szkoleń niż 100
- Szkolenia muszą być dostępne w postaci filmów, plików audio, prezentacji, broszur oraz interaktywnych gier, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
- Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:
 - Ryzyka związanego z AI
 - Bezpieczeństwa informacji
 - Klasyfikacji informacji
 - Cyklu życia informacji
 - Własności intelektualnej
 - Haseł
 - Kontroli dostępu
 - Poczty Email
 - Bezpieczeństwa w Internecie
 - Inżynierii społecznej
 - Prywatności
 - Danych płatniczych
 - Phishing
 - Malware/Wirusów/Ransomware
 - Kradzieży tożsamości
 - Mediów społecznościowych
 - Pracy zdalnej
 - Urządzeń mobilnych
 - Wycieku danych
 - Otwartych sieci WiFi
 - Usług chmurowych

- Personalnych urządzeń w organizacji (BYOD)
 - Bezpieczeństwa w podróży
- To samo szkolenie musi być dostępne zarówno w trybie wymagającym interakcji (np. odtworzenie filmu w całości by móc przejść dalej) jak i w trybie dostępnym, który nie wymaga konieczności interakcji lub ogranicza konieczność interakcji użytkownika, by ukończyć szkolenie.
- Platforma musi zapewniać również szkolenia dostosowane do wymagań WCAG.
- System musi dawać możliwość podzielenia użytkowników na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz quizów.
- Łączny czas trwania wszystkich materiałów szkoleniowych w języku polskim musi wynosić co najmniej 10 godzin.

2.2. Moduł Quizów:

- System musi pozwalać na stworzenie quizu, niezwiązanego z żadnym szkoleniem
- Quizy muszą być dostępne w trzech formatach: ogólnodostępne, tylko dla wybranych użytkowników lub dostępne za pośrednictwem bezpośredniego linku
- Administrator może wybrać czy quiz wymaga pewnej punktacji do zaliczenia czy też nie.
- Administrator może wybrać, czy quiz można powtarzać w przypadku niepowodzenia
- Pytania do quizów może tworzyć ręcznie administrator lub mogą one być zaciągane z innych modułów systemu

2.3. Moduł narzędzi dodatkowych

- Narzędzia dodatkowe muszą zawierać w sobie grafiki, ulotki, animacje, pozwalające na ich wydruk lub umieszczenie w interaktywnych elementach infrastruktury zamawiającego. Przykładem może być gif umieszczony w stopce maila, informując o zagrożeniach lub prowadzonej kampanii edukacyjnej.

2.4. Moduł raportujący obejmujący minimum:

- status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów.

3. Kursy oraz Quizy mogą zostać połączone w jedną, spójną kampanię, wykonywaną krok po kroku wedle ustalonego wcześniej harmonogramu, bez konieczności interakcji z zewnątrz

4. Wszystkie moduły (platforma zarządzająca, szkoleniowa, moduł raportowania, moduł quizów, moduł narzędzi dodatkowych) muszą pochodzić od jednego producenta i być świadczone w trybie 24/7/365.

Zadanie 2. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS

1. Przedmiot zamówienia

Przedmiotem zamówienia jest realizacja dwudniowego, stacjonarnego szkolenia specjalistycznego zakończonego certyfikatami potwierdzającymi ukończenie szkolenia dla 4 pracowników kadry w zakresie obsługi i utrzymania dostarczonych systemów cyberbezpieczeństwa oraz w zakresie dostosowania organizacji do wymogów prawnych wynikających z Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) oraz dyrektywy NIS2, ze szczególnym uwzględnieniem odpowiedzialności cywilnej, karnej i administracyjnej Zarządu oraz kadry kierowniczej.

2. Szczegółowy zakres merytoryczny

2.1. Wykonawca w ramach usługi zrealizuje następujące moduły tematyczne:

- Fundamenty prawne i zgodność (Compliance):
 - Analiza korelacji między przepisami krajowymi (KSC) a unijnymi (NIS2).
 - Wskazanie konkretnych artykułów i wymogów prawnych bezpośrednio wpływających na procesy biznesowe organizacji.
- Zarządzanie incydentami i sankcje:
 - Procedura formalno-prawna zgłaszania incydentów do właściwych organów (CSIRT).
 - Analiza ryzyk prawnych: Skutki zaniechania zgłoszeń lub ich nieterminowości.
 - Kary i SLA: Omówienie mechanizmów kar umownych oraz administracyjnych kar pieniężnych za niedotrzymanie parametrów SLA (Service Level Agreement) w umowach z dostawcami i organami nadzorczymi.
- **Odpowiedzialność Zarządu (C-Level Responsibility):**
 - Osobista odpowiedzialność członków organów zarządzających za uchybienia w nadzorze nad cyberbezpieczeństwem.
 - Obowiązek zatwierdzania środków zarządzania ryzykiem i nadzoru nad ich wdrażaniem (zgodnie z wymogami NIS2).
 - Rola Zarządu w ochronie infrastruktury krytycznej i zapewnieniu ciągłości działania.

3. Warunki logistyczne i organizacyjne

- 3.1. Miejsce szkolenia: Autoryzowane lub wyspecjalizowane centrum szkoleniowe Wykonawcy (poza siedzibą Zamawiającego).
- 3.2. Czas trwania: 2 dni robocze (łącznie min. 14-16 godzin dydaktycznych).
- 3.3. Wykonawca zapewnia:
 - Nocleg dla uczestników w standardzie min. 3* (pokój jednoosobowy lub dwuosobowy zgodnie z ustaleniami).

- Pełne wyżywienie (śniadania, obiady, kolacje oraz przerwy kawowe).
- Materiały: Każdy uczestnik otrzyma komplet materiałów szkoleniowych w formie papierowej lub elektronicznej oraz certyfikat potwierdzający ukończenie szkolenia.

Zadanie 3. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS

1. Przedmiot zamówienia

Przedmiotem zamówienia jest realizacja specjalistycznego szkolenia z zakresu cyberbezpieczeństwa dla 4 pracowników Zamawiającego. Szkolenie zostanie przeprowadzone w formie stacjonarnej w centrum szkoleniowym Wykonawcy, w wymiarze 2 dni szkoleniowych wraz z certyfikatami potwierdzającymi ukończenie szkolenia.

Zamówienie powinno być zrealizowane w cyklu dwudniowego, stacjonarnego szkolenia specjalistycznego dla kadry zarządzającej w zakresie obsługi i utrzymania dostarczonych systemów cyberbezpieczeństwa oraz wypełniania obowiązków wynikających z Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC).

2. Szczegółowy zakres merytoryczny

2.1. Program szkolenia musi obejmować następujące moduły:

- Bezpieczeństwo infrastruktury hybrydowej (IT/OT):
 - Specyfika ochrony systemów informatycznych oraz systemów automatyki przemysłowej i sterowania.
- Obowiązki i działania w ramach KSC:
 - Praktyczna realizacja obowiązków ustawowych przez operatora/właściciela systemu.
 - Procedury identyfikacji i klasyfikacji incydentów w sieciach IT oraz OT.
 - Zasady i kanały zgłaszania incydentów krytycznych do właściwych organów (CSIRT poziomu krajowego).
- Obsługa techniczna systemów zabezpieczeń:
 - Szkolenie z zakresu administracji i konfiguracji systemów NDR (Network Detection and Response)
 - Systemów zapór ogniowych (Firewall/Next-Generation Firewall).
 - Monitorowanie ruchu sieciowego pod kątem anomalii w sieciach IT/OT
- Ciągłość działania i ochrona danych:
 - Procedury tworzenia kopii zapasowych (backup).

- Praktyczna weryfikacja poprawności wykonania kopii oraz testy odtwarzania danych po awarii (Disaster Recovery).

3. Warunki logistyczne i organizacyjne

- 3.1. Miejsce szkolenia: Autoryzowane lub wyspecjalizowane centrum szkoleniowe Wykonawcy (poza siedzibą Zamawiającego).
- 3.2. Czas trwania: 2 dni robocze (łącznie min. 14-16 godzin dydaktycznych).
- 3.3. Wykonawca zapewnia:
 - Nocleg dla uczestników w standardzie min. 3* (pokój jednoosobowy lub dwuosobowy zgodnie z ustaleniami).
 - Pełne wyżywienie (śniadania, obiady, kolacje oraz przerwy kawowe).
 - Materiały: Każdy uczestnik otrzyma komplet materiałów szkoleniowych w formie papierowej lub elektronicznej oraz certyfikat potwierdzający ukończenie szkolenia.

4. Wymagania wobec trenera

- 4.1. Szkolenie powinno być prowadzone przez trenera posiadającego minimum 2 letnie udokumentowane doświadczenie praktyczne w projektowaniu i utrzymaniu oferowanych w przedmiotowym postępowaniu systemów bezpieczeństwa.(tj, NGFW,NDR,SIEM,PAM,AV,DLP, Bezpieczeństwo OT)

Zadanie 4. Wykonanie szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami IT/OT/ICS

1. Przedmiot zamówienia

Szkolenie z zakresu cyberbezpieczeństwa i kompetencji cyfrowych z wykorzystaniem technologii VR dla 22 osób w siedzibie zamawiającego

2. Cel szkolenia

2.1. Podniesienie kompetencji cyfrowych pracowników w zakresie:

- rozpoznawania cyberzagrożeń
- bezpiecznego korzystania z systemów IT
- ochrony danych osobowych i informacji wrażliwych
- reagowania na incydenty bezpieczeństwa
- budowania kultury cyberbezpieczeństwa w organizacji

2.2. Szkolenie koncentruje się na czynniku ludzkim jako kluczowym elemencie systemu bezpieczeństwa.

3. Grupa docelowa

- 3.1. pracownicy administracji publicznej
- 3.2. pracownicy spółek komunalnych (np. wodociągi, infrastruktura krytyczna)
- 3.3. kadra zarządzająca
- 3.4. pracownicy operacyjni korzystający z systemów IT

Nie jest wymagane wykształcenie techniczne.

4. Forma realizacji

- 4.1. Szkolenie stacjonarne w formule warsztatowej z wykorzystaniem:
 - okularów VR (np. Pico / Meta)
 - autorskich aplikacji szkoleniowych symulujących incydenty cyberbezpieczeństwa
 - scenariuszy decyzyjnych (Red/Blue Team w wersji edukacyjnej) - minimum 13 unikalnych scenariuszy w tym SOC, NIS2 i ASI.
 - case studies opartych na realnych atakach
 - materiałów drukowanych (checklisty, komiksy edukacyjne, scenariusze sytuacyjne)

5. Zakres merytoryczny

- 5.1. Blok I – Aktualne zagrożenia cybernetyczne
 - phishing i spear phishing
 - ransomware
 - socjotechnika
 - ataki na infrastrukturę krytyczną
 - zagrożenia wewnętrzne
- 5.2. Blok II – Symulacje VR
 - Uczestnik w środowisku wirtualnym:
 - podejmuje decyzje podczas symulowanego ataku phishingowego
 - analizuje skutki kliknięcia w złośliwy link
 - reaguje na próbę wyłudzenia danych
 - doświadcza konsekwencji błędnych decyzji w kontrolowanym środowisku
- 5.3. Blok III – Ochrona danych i odpowiedzialność pracownika
 - podstawy ochrony danych osobowych
 - bezpieczeństwo informacji w pracy administracyjnej
 - dobre praktyki haseł i MFA
 - praca zdalna i mobilna – zasady bezpieczeństwa
- 5.4. Blok IV – Procedury reagowania
 - jak zgłaszać incydenty
 - co robić, a czego nie robić w pierwszych minutach
 - odpowiedzialność organizacyjna

6. Wymiar godzinowy

- 6.1. Standardowy moduł:
 - 6–7 godzin zegarowych (1 dzień szkoleniowy)
- 6.2. Możliwa realizacja w wariantach:

- 4h (wersja skrócona)
- 2 dni (wariant rozszerzony z dodatkowymi scenariuszami VR)

7. Liczebność grupy

- Optymalnie: 12–20 osób
- Przy większych grupach – rotacyjna praca na stanowiskach VR.

8. Efekty szkolenia

8.1. Uczestnik:

- rozumie mechanizmy ataków cybernetycznych
- potrafi rozpoznać próbę manipulacji
- zna zasady bezpiecznego przetwarzania informacji
- wie jak reagować w sytuacji incydentu
- ma zwiększoną świadomość wpływu własnych decyzji na bezpieczeństwo organizacji

9. Wyróżnik szkolenia:

- 9.1. wykorzystanie immersyjnej technologii VR
- 9.2. realne symulacje zamiast samej prezentacji
- 9.3. doświadczenie konsekwencji błędów bez realnego ryzyka
- 9.4. wysoki poziom zaangażowania uczestników
- 9.5. praktyczne podejście zamiast teoretycznego wykładu

Zadanie 5. Usługi typu security awareness do symulowanych ataków socjotechnicznych IT/OT/ICS dostępu do portalu dla pracowników Zamawiającego.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostępu do portalu w formie usługi, umożliwiającego przeprowadzenia wielu kampanii phishingowych przy codziennych obowiązkach.

- 1.1. Wykonawca musi dostarczyć platformę dedykowaną użytkownikom Zamawiającego i świadczoną przez okres min. do 30.06.2026 r.
- 1.2. Platforma musi być dostępna za pomocą dowolnej, nowoczesnej przeglądarki internetowej (Chrome, Firefox, Edge) a sama usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej.
- 1.3. Dostęp dla użytkownika musi odbywać się minimum w języku polskim, angielskim oraz trzecim wybranym przez Zamawiającego języku
- 1.4. Podczas tworzenia użytkownika, musi być możliwość wyboru domyślnego języka, w którym będzie on otrzymywał kampanie phishingowe. Niedopuszczalnym jest konieczność tworzenia osobnej kampanii phishingowej per każdy z dostępnych dla Zamawiającego języków.

2. Wymagania dotyczące platformy phishingowej:

Usługa musi zawierać poszczególne komponenty:

- 2.1.** Platforma phishingowa pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi (wedle ich domyślnego języka) oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:
- z linkiem prowadzącym do stronnym internetowej,
 - z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
 - z załącznikiem zawierającym potencjalnie niebezpieczny kod,
 - z załącznikiem w postaci dokumentu Word, Excel, PowerPoint, PDF, ZIP zawierającym potencjalnie niebezpieczny kod
- 2.2.** W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.
- 2.3.** Maile phishingowe muszą mieć możliwość dystrybucji w czasie, tak by nie wszyscy użytkownicy dostali tą samą wiadomość w jednej chwili.
- 2.4.** Platforma musi posiadać rozbudowaną bazę szablonów maili oraz stron phishingowych, co najmniej maili pochodzących od:
- Microsoft/Office365
 - Microsoft/Teams
 - Microsoft/Sharepoint
 - Microsoft/OneDrive
 - DHL
 - Limitu skrzynki pocztowej
 - Zoom
 - Google Drive
 - Apple
- 2.5.** Platforma musi pozwalać na wgranie własnego szablonu wiadomości Email
- 2.6.** Moduł raportujący obejmujący minimum:
- status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, kto wpisał dane w formularzu jaka była platforma oraz przeglądarka z której wykonał tę akcję oraz szczegółowe daty wykonania tych operacji.
- 2.7.** Symulacje phishingu mogą być wykonywane wedle ustalonego wcześniej harmonogramu, bez konieczności interakcji z zewnątrz

Platforma phishingowa musi być świadczona w trybie 24/7/365.

Zadanie 6. Oprogramowanie do badania podatności

1. Przedmiot zamówienia

Przedmiotem dostawy jest dostarczenie 30 sztuk oprogramowania wraz z kompletem licencji niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego. Subskrypcja ważna minimum do dnia 30.06.2026

2. Wymagania dotyczące oprogramowania

2.1. W ramach zadania Wykonawca dostarczy licencje na oprogramowanie dla stacji roboczych i serwerów

2.2. Parametry minimalnych wymagań oprogramowania posiadającego funkcjonalność skanera podatności, patch managera oraz platformy do zarządzania podatnościami:

- Platforma musi być oparta na chmurze (SaaS).
- Konsola wymaga dostępu przeglądarki Web do Internetu w celu podglądu złośliwych treści i/lub podatności, obejmując analizę, prewencję oraz informacje o reakcji na malware.
- Platforma musi skanować i wykrywać złośliwe treści i/lub luki w zabezpieczeniach dla co najmniej 1000 adresów IP (hostów) online.
- Platforma musi zapewniać widoczność i pokrycie w czasie rzeczywistym dla systemów operacyjnych i aplikacji w organizacji.
- Wszelkie zmiany w inwentarzu (instalacja/deinstalacja/zmiana aplikacji lub zasobów) muszą być natychmiast odzwierciedlane w konsoli.
- Platforma/konsola musi oferować zintegrowane rozwiązanie do zarządzania podatnościami, priorytetyzacji ryzyka oraz remediacji.
- Platforma musi działać na jednym z najczęściej używanych dostawców usług w chmurze.
- Platforma/konsola musi obsługiwać co najmniej dwie metody uwierzytelniania (np. nazwa użytkownika i hasło, e-mail weryfikacyjny, SAML2 z IDP).
- Platforma musi obsługiwać wdrażanie proxy sieciowego do buforowania poprawek.
- Proxy musi działać w systemie Linux Ubuntu lub Red Hat i nie może generować dodatkowych kosztów.
- W przypadku infekcji złośliwym oprogramowaniem skrypty muszą izolować zagrożone systemy, eliminować złośliwe procesy oraz szybko i skutecznie przywracać bezpieczne konfiguracje.
- Niestandardowe skrypty muszą umożliwiać wykrywanie luk w zabezpieczeniach i podejrzanych urządzeń.
- Generatywna sztuczna inteligencja musi analizować historyczne i bieżące wzorce danych w celu identyfikacji pojawiających się zagrożeń i potencjalnych infekcji złośliwym oprogramowaniem.
- Platforma musi zapewniać proaktywną ochronę przed pojawiającymi się

zagrożeniami.

- Platforma musi zawierać mechanizmy wczesnego wykrywania wykorzystujące sztuczną inteligencję i aktualne źródła informacji, aby wyprzedzać atakujących.
- Platforma musi dostarczać automatyczne aktualizacje zabezpieczeń w celu przeciwdziałania nowym lukom i zagrożeniom bez ręcznej interwencji, stosowane płynnie i bez konfliktów.
- Platforma musi oferować szczegółowe funkcje audytu i konfigurowalnego raportowania, obsługiwane przez API, z wyraźną widocznością stanu bezpieczeństwa.
- Platforma musi wspierać aplikacje na systemie operacyjnym.
- Platforma musi posiadać konfigurowalny model ryzyka.
- Platforma musi w sposób ciągły oceniać złośliwe treści i/lub luki w zabezpieczeniach.
- Platforma w sposób automatyczny musi rozpoznawać aplikacje.
- Priorytetyzacja zagrożeń musi być oparta o zasoby.
- Priorytetyzacja luk w zabezpieczeniach musi być wykonywana w połączeniu z informacjami wewnętrznymi.
- Platforma musi zapewniać scentralizowaną priorytetyzację podatności i usuwanie zagrożeń z poziomu jednej konsoli.

2.3. Klasyfikacja ryzyk:

- Platforma musi posiadać proces klasyfikacji ryzyka służący do priorytetyzacji remediacji wykrytych podatności.
- Platforma musi klasyfikować ryzyko w oparciu o zasoby.
- Platforma musi klasyfikować ryzyko w oparciu o aplikacje.
- Platforma musi prezentować klasyfikację ryzyka i priorytetyzować podatności nie tylko na podstawie poziomu zagrożenia CVE, ale także czynników kontekstowych, takich jak warunki środowiskowe.
- Platforma musi mapować priorytety.
- Platforma umożliwia patch management dla systemów operacyjnych Windows.
- Platforma umożliwia patch management dla aplikacji działających na systemie operacyjnym Windows od firm trzecich.
- Platforma umożliwia patch management systemów operacyjnych dla Linux.
- Platforma umożliwia patch management dla aplikacji działających na systemie operacyjnym Linux od firm trzecich.
- Platforma umożliwia patch management dla systemów operacyjnych macOS.
- Platforma umożliwia patch management dla aplikacji działających na systemie operacyjnym macOS od firm trzecich.
- Platforma musi zapewniać wykrywanie podatności w czasie rzeczywistym.
- Platforma musi zapewniać ochronę przed wykorzystaniem podatności w czasie rzeczywistym z w przypadku braku dostępnego patcha.
- Platforma musi zapewniać ochronę przed podatnościami typu Process Memory

Scrapping, Direct API Abuse lub Process Impersonation bez konieczności stosowania patcha.

- Platforma musi dostarczać szczegółowe informacje o każdym CVE.
- Platforma musi zapewniać aktualizacje podatności w czasie rzeczywistym.
- Platforma musi obsługiwać co najmniej 160 000 podatności typu legacy zarejestrowanych w NIST.
- Platforma musi umożliwiać wykonywanie komend na wszystkich stacjach końcowych z agentem.
- Platforma musi identyfikować poprawki zabezpieczeń systemów operacyjnych.
- Platforma musi umożliwiać planowanie instalacji aktualizacji lub wykonywania skryptów.
- Platforma musi umożliwiać uruchamianie wstępnie skonfigurowanych i dostosowanych do indywidualnych potrzeb automatycznych działań.
- Platforma musi umożliwiać tworzenie skryptów dla Windows, Linux i macOS.
- Platforma musi zapewniać ochronę przed podatnościami typu zero-day.
- Platforma musi posiadać mechanizm rekomendacji działań wspierający administratorów przy wyborze reakcji.
- Platforma musi zawierać szablony skryptów dla zadań Red Team i Blue Team.
- Platforma musi integrować się z technologiami AI do automatycznej remediacji podatności.
- Platforma musi udostępniać szablony skryptów dla zespołów SysAdmin.
- Platforma musi wykonywać skrypty wykrywania i remediacji dla CVE.
- Agent musi umożliwiać wdrożenie z poziomu command line.
- Agent musi umożliwiać wdrożenie za pomocą GPO.
- Platforma musi obsługiwać wiele ról użytkowników.
- Platforma musi umożliwiać podział zasobów pomiędzy grupy użytkowników z różnymi poziomami uprawnień.
- Agent musi umożliwiać skanowanie i patchowanie Windows, Linux oraz macOS.
- Platforma musi umożliwiać wdrożenie na co najmniej 1 000 hostów online.
- Agent musi zapewniać możliwość samodzielnej aktualizacji.
- Platforma musi obsługiwać integracje z systemami typu SIEM (np. Splunk, SumoLogic).
- Platforma musi obsługiwać integracje z dowolnym oprogramowaniem poprzez API.
- Platforma musi obsługiwać integracje SAML2 z dostawcami tożsamości (np. Okta, Ping Identity).
- Platforma musi umożliwiać generowanie raportów podatności w formatach takich jak PDF oraz eksport CSV.
- Platforma musi posiadać dashboard prezentujący wyniki podatności w czasie rzeczywistym.
- Raporty ryzyka muszą być dostępne w konsoli.
- Platforma musi umożliwiać raportowanie ryzyka dla wielu aplikacji.

- Platforma musi zapewniać zewnętrzne narzędzie raportowe do generowania wykresów remediacji oraz monitorowania KPI.
- Platforma musi integrować się z zewnętrznymi narzędziami skanowania sieci (np. Nmap).

Zadanie 7. Oprogramowanie do ochrony przed ransomware

1. Przedmiot zamówienia

Przedmiotem dostawy jest dostarczenie 30 sztuk oprogramowania wraz z kompletem licencji niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego. Subskrypcja ważna minimum do dnia 30.06.2026

2. Wymagania dotyczące oprogramowania

2.1. Konsola zarządzająca

- Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.
- Konsola web administratora musi posiadać możliwość wyboru języka polskiego
- Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.
- Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi i odrębnie między urządzeniami mobilnymi
- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.
- Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.
- Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.

- Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.
- Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach bezpośrednio z bezpiecznego repozytorium dostawcy rozwiązania antywirusowego.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.
- Konsola web umożliwia zmianę ustawień priorytetu skanowania.
- Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.
- Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.
- Konsola web musi umożliwiać synchronizację z Azure Active Directory.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z aplikacji zainstalowanej na stacji klienckiej.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.
- Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.

2.2. Zarządzanie użytkownikami i stacjami

- System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu.
- System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit.
- Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows.
- Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkownika przez administratora w określonym przez niego czasie.
- Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkownika przez administratora w celu odpytania go o zgodę na połączenie.
- Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli.
- Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

2.3. Agent ochrony konsoli oprogramowanie antywirusowe

- Program antywirusowy powinien mieć obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:

- macOS:
 - 10.14.x
 - 10.15.x
 - 11.x
 - 12.x
 - 13.x
 - 14.x
 - 15.x
- MS Windows (stacje klienckie):
 - Windows XP (SP3 or higher) x86
 - Windows 7 SP1 x86
 - Windows 7 SP1 x64
 - Windows 8 x86
 - Windows 8 x64
 - Windows 8.1 x86
 - Windows 8.1 x64
 - Windows 10 x86
 - Windows 10 x64
 - Windows 11 x64
- MS Windows (wersja serwerowa):
 - Windows Server 2003 SP2
 - Windows Server 2003 R2 SP2
 - Windows Server 2008 SP2
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
 - Windows Server 2025
- LinuxOS z gwarantowaną kompatybilnością:
 - Latest Ubuntu 16.x LTS x64 release version (with GUI)
 - Latest Ubuntu 18.x LTS x64 release version (with GUI)
 - Latest Ubuntu 19.x x64 release version (with GUI)
 - Latest Ubuntu 20.x LTS x64 release version (with GUI)
 - Latest Ubuntu 21.04 x64 release version (with GUI)
 - Latest Ubuntu 22.04 x64 release version (with GUI)
 - Latest Debian 8.x x64 release version (with GUI)
 - Latest Debian 9.x x64 release version (with GUI)
 - Latest Debian 10.x x64 release version (with GUI)
 - Latest Red Hat Enterprise Linux Server 7.x x64 release version (with GUI)

- Latest Red Hat Enterprise Linux Server 8.x x64 release version (with GUI)
- Latest CentOS 7.x x64 release version (with GUI)
- Latest CentOS 8.x x64 release version (with GUI)
- Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:
 - 512 MB dostępnej pamięci RAM
 - 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej
- Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.
- Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox).
- Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji.
- Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB
- Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych.
- Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym.
- Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze.
- Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje.
- Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa).
- Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym.
- Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie).
- Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu antywirusowego.
- Podczas pracy komputera Program musi automatycznie skanować:
 - pliki uruchamiane, otwierane,
 - pliki kopiowane lub przenoszone,
 - pliki tworzone,
 - pliki pobierane z Internetu po protokole HTTP/HTTPS.

- W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów.
- Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS.
- Program antywirusowy powinien posiadać dodatkowe narzędzie do skanowania systemu.
- Program antywirusowy musi posiadać dodatkowe narzędzie do analizowania bezpieczeństwa procesów.
- Program antywirusowy powinien mieć możliwość skanowania skompresowanych plików.
- Program antywirusowy musi być z możliwością zablokowania dostępu do zmiany ustawień programu hasłem administratora oraz hasłem skonfigurowanym w konsoli zarządzającej.
- Program antywirusowy powinien mieć możliwość importowania oraz eksportowania ustawień.
- Program antywirusowy powinien mieć możliwość tworzenia list zaufanych procesów.
- Program antywirusowy powinien mieć możliwość tworzenia list zaufanych plików.
- Program antywirusowy i konsola powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików.
- Program antywirusowy powinien umożliwiać konfigurację polityk (globalnych ustawień dla grup endpointów) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń.
- Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania.
- Program antywirusowy powinien umożliwiać skanowanie pamięci komputera po uruchomieniu.
- Program antywirusowy posiada zintegrowaną funkcję skanowania i ochrony plików pod kątem danych wrażliwych.
- Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie.
- Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych.
- Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu.
- Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowane od reszty systemu operacyjnego i mieć możliwość uruchomienia takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych.
- Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.

- Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (windows)
- Oprogramowanie chroni przed nieupoważnionym zrzutem obrazu z ekranu.
- Oprogramowanie umożliwia analizę skryptu w programach pod kątem złośliwego oprogramowania przed ich uruchomieniem.
- Oprogramowanie umożliwia na rejestrowanie dzienników zdarzeń oraz zapisywanie ich lokalnie i na zewnętrznym serwerze.
- Oprogramowanie umożliwia personalizację wyglądu agenta ochrony.
- Oprogramowanie umożliwia zastosowanie proxy do rozpropagowania aktualizacji wewnątrz sieci.
- Oprogramowanie umożliwia procentową regulację zużycia zasobów procesora oraz nadania priorytetu.
- Oprogramowanie umożliwia śledzenie bibliotek uruchomionych przez procesy oraz blokowanie nieznanych bibliotek.

2.4. Dodatkowe systemy bezpieczeństwa

- Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach.
- Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci.

Zadanie 8. Oprogramowanie typu EDR (Endpoint Detection and Response)

1. Przedmiot zamówienia

Przedmiotem dostawy jest 30 sztuk oprogramowania wraz z kompletem licencji na niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego. Subskrypcja ważna minimum do dnia 30.06.2026

2. Wymagania dotyczące oprogramowania:

2.1. Konsola zarządzająca:

- Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.
- Konsola web administratora musi posiadać możliwość wyboru języka polskiego
- Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.

- Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi i odrębnie między urządzeniami mobilnymi
- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.
- Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.
- Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.
- Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.
- Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach bezpośrednio z bezpiecznego repozytorium dostawcy rozwiązania antywirusowego.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.
- Konsola web umożliwia zmianę ustawień priorytetu skanowania.
- Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.
- Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.
- Konsola web musi umożliwiać synchronizację z Azure Active Directory.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z aplikacji zainstalowanej na stacji klienckiej.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.
- Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.

2.2. Wymagania techniczne oraz obsługiwane systemy:

- Platforma systemu EDR powinna posiadać obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:
 - MS Windows (stacje klienckie):
 - Windows 7 SP1 x86
 - Windows 7 SP1 x64

- Windows 8 x86
- Windows 8 x64
- Windows 8.1 x86
- Windows 8.1 x64
- Windows 10 x86
- Windows 10 x64
- Windows 11 x64
- MS Windows (wersja serwerowa):
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
 - Windows Server 2025
- Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:
 - 512 MB dostępnej pamięci RAM
 - 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej
- Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.

2.3. Wymagania funkcjonalności systemu EDR

- Platforma systemu EDR powinna posiadać obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:
 - MS Windows (stacje klienckie):
 - Windows 7 SP1 x86
 - Windows 7 SP1 x64
 - Windows 8 x86
 - Windows 8 x64
 - Windows 8.1 x86
 - Windows 8.1 x64
 - Windows 10 x86
 - Windows 10 x64
 - Windows 11 x64
 - MS Windows (wersja serwerowa):
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
 - Windows Server 2025
- Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:
 - 512 MB dostępnej pamięci RAM
 - 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej
- Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.

- Rozwiązanie zawiera w sobie moduł oparty na technologii typu "Endpoint Detection & Response", zwany dalej EDR.
- System EDR ma funkcję śledzenia zdarzeń systemowych i sieciowych urządzeń na których jest wdrożony.
- System EDR musi posiadać moduł chroniący urządzenia w czasie rzeczywistym.
- System EDR powinien posiadać narzędzie do skanowania systemu.
- System EDR powinien chronić urządzenia przed zaawansowanymi zagrożeniami w tym między innymi: „trojan”, „ransomware”, „malware”, „dialer”, „keylogger”, „adware”, „greyware”, „spyware”.
- Pozwolić administratorom odszukać informację dotyczące incydentów związanych z bezpieczeństwem, zapewniając wgląd w zakres ataku, sposób jego rozpoczęcia, wpływ i sposób reagowania,
- Nawiązanie zdalnego połączenia ze stacją końcową poprzez zdalną powłokę bezpośrednio z konsoli systemu lub z wykorzystaniem Powershell/cmd/bash:
 - Przeglądanie zawartości stacji końcowej (listowanie plików/katalogów),
 - Wyświetlanie zmiennych środowiskowych,
 - Wyświetlanie konfiguracji sieci,
 - Wyświetlanie aktualnych połączeń sieciowych,
 - Wyświetlanie listy procesów,
 - Przeglądanie kluczy rejestrów i ich wartości,
 - Wyświetlanie listy usług, wraz ze statusem,
 - Wyświetlanie listy użytkowników,
 - Zakończenie procesu,
 - Usunięcie pliku/folderu,
 - Pobranie pliku.
- Podczas pracy urządzenia system EDR musi automatycznie skanować:
 - pliki uruchamiane, otwierane,
 - pliki kopiowane lub przenoszone,
 - pliki tworzone,
 - pliki pobierane z Internetu po protokole HTTP/HTTPS.
- System EDR ma funkcję tworzenia alertów wybranych zdarzeń, typowanych na stanowiące potencjalne zagrożenie dla bezpieczeństwa urządzenia zgodnie z przyjętą polityką.
- System EDR powinien pozwalać zarządzać statusem alertu:
 - Nowy
 - Zamknięty
- Polityka bezpieczeństwa musi być edytowalna i mieć możliwość wprowadzania samodzielnie zdefiniowanych reguł. Nie jest dopuszczalne ograniczenie do reguł predefiniowanych przez producenta.
- Funkcja śledzenia zdarzeń musi mieć możliwość ich filtrowania względem co najmniej 10-ciu parametrów, w szczególności:

- urządzenia
- użytkownika
- podsystemu bezpieczeństwa
- techniki potencjalnego ataku.
- taktyki potencjalnego ataku.
- Moduł EDR musi mieć możliwość korelacji ewentualnych powiązań pomiędzy śledzonymi zdarzeniami i przedstawienia ich z użyciem sygnatur czasowych i/lub na osi czasu.
- Korelacja zdarzeń śledzonych przez EDR ma dotyczyć w szczególności:
 - zmian w plikach
 - zmian w rejestrze systemowym
 - działających procesów i podprocesów
 - dostępu do urządzeń zewnętrznych
- System EDR musi chronić stacje poprzez uruchamianie nieznanego oraz niebezpiecznych załączników znajdujących się w wiadomościach pocztowych e-mail.
- System EDR musi wykrywać i reagować na zagrożenia wykryte w podłączonych zewnętrznych nośnikach danych takich jak dyski, pendrive, modemy.
- System EDR musi posiadać moduł sprawdzający reputację plików w chmurze.
- System EDR musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu.
- System EDR powinien mieć możliwość skanowania skompresowanych plików.
- System EDR powinien umożliwiać tworzenie wyjątków ze skanowania folderów / plików.
- System EDR powinien pozwalać na podejmowanie akcji w szczególnych zdarzeniach:
 - Izolacja stacji końcowej
 - Uruchomienie skryptu
- System EDR umożliwia rejestrowanie dzienników zdarzeń oraz zapisywanie ich lokalnie i na zewnętrznym serwerze.
- System umożliwia śledzenie bibliotek uruchomionych przez procesy oraz blokowanie nieznanego bibliotek.
- Umożliwiać wyszukiwanie szczegółów dotyczących wykonanych poleceń w PowerShell na punktach końcowych,

2.4. Dodatkowe systemy bezpieczeństwa

- Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach.
- Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci.

2.5. Dostawa, gwarancja i usługa wdrożeniowa

- Dostawca zapewni wdrożenie rozwiązania u Zamawiającego w terminie nie późniejszym niż do 60 dni od podpisania umowy.
- Licencja na oprogramowanie powinna mieć charakter subskrypcyjny.
- Dostawa musi zawierać również:
 - Wsparcie techniczne dystrybutora rozwiązania w języku polskim świadczone przez dział techniczny posiadający odpowiednie kompetencje potwierdzone posiadanymi certyfikatami na poziomie ekspert.
 - Szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez producenta lub dystrybutora oferowanego rozwiązania w języku polskim.
- Oferta musi być złożona przez autoryzowanego partnera producenta/dystrybutora posiadającego niezbędne kompetencje do zrealizowania zamówienia.

Zamawiający dopuszcza rozwiązanie równoważne różnych producentów zgodne z opisem przedmiotu zamówienia pod warunkiem iż będą one posiadać jedną centralną konsolę do zarządzania wszystkimi komponentami systemu oraz będą obsługiwane przez jedno centralne wsparcie techniczne w języku Polskim

Zadanie 9. Urządzenie i oprogramowanie typu NDR z HoneyPot i monitorem sytuacyjnym (Network Detection & Response)

1. Przedmiot zamówienia

Przedmiotem dostawy jest dostarczenie 1 sztuki urządzenia NDR z HoneyPot wraz z kompletem licencji niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego oraz dostarczenie 1 sztuki monitora sytuacyjnego.

2. Wymagania dotyczące rozwiązania:

2.1. Minimalne parametry techniczne i funkcjonalne NDR:

- Elementy systemu bezpieczeństwa
 - Wysokość 1U do montażu w szafie rack.
 - Posiadać co najmniej dwa porty USB
 - Urządzenie musi posiadać dedykowany port do zarządzania
 - Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE
 - Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
 - Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń
 - Proponowane rozwiązanie musi obsługiwać minimum 750 tys. jednoczesnych sesji.
 - Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
- Usługi sieciowe
 - Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.

- Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń
- Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
- Kontrola aplikacji
 - Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimedialnych itp.
 - Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
 - Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
- Wykrywanie zagrożeń
 - Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
 - Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6
 - Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
 - Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
 - Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
 - Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
 - Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
 - Rozwiązanie musi mieć opcję przechwytywania pakietów
 - Rozwiązanie musi umieć wykrywać reverse-shell
 - Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu
 - System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
- Skanowanie antywirusowe
 - Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
 - Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
 - Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach

- Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
- Wykrywanie botnetów C&C
 - Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
 - Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C
 - Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
 - Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
 - Rozwiązanie musi wspierać włączenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
 - Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
- Sandbox w chmurze
 - Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanymi zagrożeń
 - Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
 - Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
 - Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR, SWF oraz skrypty
 - Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików.
 - Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznanne zagrożenie.
- Wykrywanie spamu
 - Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym
 - Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
 - Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3
 - Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
- Dodatkowe funkcje ochrony
 - Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
 - Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP
 - Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
 - Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
- Inteligentne funkcje bezpieczeństwa

- Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
- Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
- Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp
- Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania
- Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
- Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.
- Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS
- Rozwiązanie musi obsługiwać inspekcję zaszyfowanego ruchu tunelowego dla nieznanymi aplikacji
- Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym
- Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
- Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia
- Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta
- Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
- Rozwiązanie musi obsługiwać przechwytywanie pakietów online
- Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania
- Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych
- Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę
- Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote decto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalności funkcji śledzenia zagrożeń.
- Widoczność ryzyka/zagrożeń
 - Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.

- Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
- Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
- Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
- Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
- Rozwiązanie musi wspierać wskazanie ścieżki ataku.
- Analiza i odpowiedzi na incydenty
 - Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury
 - Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
 - Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
 - Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
 - Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail).
- Administracja
 - Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI)
 - Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli
 - Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło
 - Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
 - Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych
 - Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny
 - Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
- Logowanie i raportowanie
 - Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.

- Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
- Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
- Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
- Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje
- Wstępnie zdefiniowane zadania raportowania
- Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni.
- Rozwiązanie musi wspierać restAPI
- Gwarancja – Dostawa musi zawierać również
 - 24-miesięczną gwarancję producenta na dostarczone elementy systemu
 - Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum do 30.06.2026 (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
 - Wsparcie techniczne dystrybutora rozwiązań w języku polskim świadczone przez certyfikowanych inżynierów przez producenta na poziomie profesjonal
 - Szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania w języku polskim
 - Dostarczony sprzęt musi zostać wdrożony przez Inżyniera posiadającego najwyższy certyfikat Producenta oferowanego rozwiązania
 - Oferta musi być złożona przez autoryzowanego partnera

2.2. Minimalne parametry techniczne Monitora Sytuacyjnego

- Przekątna ekranu: wymagana przekątna matrycy nie mniejsza niż 55 cali.
- Sposób montażu: urządzenie musi być przystosowane do montażu ściennego.
- Łączność bezprzewodowa: wymagane wbudowane Wi-Fi.
- Pamięć operacyjna i wewnętrzna: urządzenie musi być wyposażone w co najmniej 4 GB pamięci RAM oraz minimum 32 GB pamięci wbudowanej.
- System operacyjny: wymagany system Android w wersji 14 lub nowszej.
- Rodzaj matrycy: wymagana matryca o powierzchni matowej.

Zadanie 10. Zaprojektowanie i wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT. Profesjonalna usługa wdrożenia rozwiązań

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie profesjonalnej usługi wdrożenia zrealizowane na bazie Projektu Wykonawczego. Zamówienie obejmuje systemy klasy komercyjnej oraz rozwiązania typu Open Source w środowiskach IT,

2. Zakres i harmonogram prac

2.1. Wykonawca zobowiązany jest do realizacji wdrożenia w terminie **60 dni roboczych** od daty dostarczenia niezbędnych komponentów (sprzętu/oprogramowania) do siedziby Zamawiającego.

2.2. Szczegółowy zakres prac obejmuje:

- Montaż i instalacja: Fizyczny montaż urządzeń w szafach RACK lub na szynach DIN oraz instalacja oprogramowania w istniejącej infrastrukturze IT Zamawiającego.
- Konfiguracja: Dostosowanie parametrów pracy rozwiązań zgodnie z wytycznymi projektowymi oraz najlepszymi praktykami bezpieczeństwa (tzw. *hardening*).
- Integracja: Zapewnienie pełnej interoperacyjności wdrażanych rozwiązań z obecnym ekosystemem sieciowym i systemowym.
- Testy akceptacyjne: Przeprowadzenie testów funkcjonalnych oraz testów bezpieczeństwa potwierdzających poprawność działania i szczelność rozwiązania.

3. Dokumentacja powdrożeniowa

3.1. W ramach zakończenia prac Wykonawca dostarczy dokumentację, który musi zawierać:

- Szczegółowy opis urządzeń: Wykaz numerów seryjnych, wersji oprogramowania (firmware), ról w systemie oraz danych dostępowych (przekazanych w sposób bezpieczny).
- Schemat fizyczny: Odzwierciedlenie rzeczywistego połączenia kablowego, lokalizacji w szafach/objektach oraz wykorzystanych portów.
- Schemat logiczny: Wizualizacja przepływu danych, adresacji IP, podziału na VLAN-y oraz reguł komunikacyjnych (szczególnie na styku IT/OT).

4. Wymagania wobec Wykonawcy (Kluczowe aspekty)

4.1. Bezpieczeństwo ciągłości procesów: Prace w środowiskach OT/ICS muszą być prowadzone w sposób niezakłócający procesów technologicznych.

4.2. Potwierdzone minimalne 4 letnie doświadczenie oraz certyfikat na poziomie profesjonal z wdrażanych rozwiązań bezpieczeństwa będących przedmiotem postępowania

4.3. Standardy: Wdrożenie musi być zgodne z obowiązującymi normami bezpieczeństwa przemysłowego (np. seria IEC 62443 lub ISO/IEC 27001).

Zadanie 11. System typu NGFW dla sieci IT HA

1. Przedmiot zamówienia

Przedmiotem dostawy są 2 sztuki urządzeń wraz z kompletem licencji niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego.

2. Wymagania dotyczące rozwiązania:

2.1. Elementy systemu bezpieczeństwa

- Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
- Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
- W zakresie Firewall, obsługa nie mniej niż 2 100 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
- Możliwość rozszerzenia pamięci do 2 TB poprzez dodatkowy dysk SSD
- Musi posiadać 2x USB 3.0 z przodu urządzenia
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
- System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości
- Systemy wirtualne muszą obsługiwać QOS
- System pełniący funkcję zapory musi posiadać nie mniej niż: 2x SFP+, 8x SFP, 8x GE interfejsów

2.2. Funkcjonalności

- Kontrola dostępu - zaporą sieciową Stateful Inspection
- Ochrona przed wirusami - komercyjny antywirus [AV]
- Poufność danych - IPSec VPN i SSL VPN
- Kontrola witryn sieci Web - filtr URL
- Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3)
- Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN
- Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
- Reputacja IP
- Cloud Sandbox

2.3. Wydajność

Wydajność dla 1 sztuki urządzenia:

- Analiza ruchu szyfrowanego protokołem SSL
- Wydajność Firewall co najmniej 10 Gb/s
- Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 3 Gb/s

- Wydajność w trybie NGFW Throughput (dla ruchu Enterprise Mix) minimum 5 Gbps
- Wydajność ochrony przed atakami (IPS) minimum 8Gb/s
- Wydajność AV nie mniej niż 5Gb/s
- Wydajność IPSec VPN, nie mniej niż 5 Gb/s

2.4. Funkcjonalności VPN

- Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
- Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
- Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności
- Praca w topologiach Hub and Spoke i Mesh
- Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,
- Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24
- Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
- Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance)
- Obsługa PnPVPN (Plug and Play VPN)

2.5. Routing

- Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
- Obsługa Policy Based Routing
- Funkcjonalność Virtual Wire

2.6. Translacja adresów NAT

- Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
- Obsługa NAT46, NAT64, DNS64
- Wsparcie dla STUN

2.7. Polityka bezpieczeństwa systemu

- Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
- Możliwość budowania min. 11000 polityk
- Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
- Musi być w stanie skonfigurować agregowane polityki
- Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)

2.8. Wydzielenie stref bezpieczeństwa

- Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
- Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
- Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników

2.9. Ochrona antywirusowa

- Silnik antywirusowy musi być oparty na przepływie tzw. flow-based

- Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV
- Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB
- Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2,
- TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji

2.10. Równoważenie obciążenia

- Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
- Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin
- Kontrola stanu serwera, monitorowanie sesji i ochrona sesji

2.11. Ochrona IPS

- Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.
- Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
- Funkcjonalność zapobiegania atakom SQL injection, XSS injection
- Możliwość budowania własnych niestandardowych reguł IPS

2.12. Obrona przed atakiem

- Ochrona przed nieprawidłowym działaniem protokołu Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
- Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
- Biała lista docelowych adresów IP

2.13. Kontrola aplikacji

- Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP.
- Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka

2.14. Filtr adresów URL

- Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
- Możliwość zdefiniowania własnej bazy kategorii www.
- Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
- Kategoria takie jak hazard, malware, spam, botnety
- Obsługa Safe Search
- Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne

- Dostosowanie strony ostrzeżenia
- 2.15. Ochrona danych**
 - Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
 - Identyfikacja protokołu pliku, w tym HTTP, FTP, SMTP, POP3, IMAP
 - Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
 - Filtrowanie plików przesyłanych przez SMB
- 2.16. Reputacja IP**
 - Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamery, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force
 - Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP
- 2.17. Zapobieganie botnetom**
 - Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
 - Wsparcie DNS sinkhole
 - Wsparcie wykrywania tunelowania DNS
 - Wyrwanie i blokowanie DGA
- 2.18. Cloud Sandbox**
 - Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń
 - Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
 - Obsługa typów plików: PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
 - Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń.
- 2.19. Uwierzytelnianie użytkownika**
 - System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu
 - Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP
 - Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazy danych
 - Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
 - Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory
 - Wsparcie usług terminalowych
 - Uwierzytelnianie użytkownika przez Web przed dotęciem do internetu
 - Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny
- 2.20. Raportowanie i przeglądanie logów**
 - Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie

- W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
- Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego
- Generowanie co najmniej 10 rodzajów raportów

2.21. System logowania

- Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.

2.22. Certyfikaty

- Rozwiązanie musi:
 - posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
 - być pozycjonowanym w raporcie Gartnera nie dalej niż ostatnie 7 lat

2.23. Zarządzanie

- Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
- Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
- Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola
- W celu rozbudowy oraz integralności systemu bezpieczeństwa urządzenie musi pochodzić od tego samego producenta co SBDS, XDR, NIPS i umożliwiać zarządzanie wszystkimi urządzeniami z chmury producenta
- Urządzenie powinno monitorować i graficznie prezentować stan pracy urządzenia. Parametry takie jak obciążenie CPU oraz pamięć z podziałem na procesy, wykres zajętości dysku twardego w czasie, temperaturę urządzenia w wybranym przez administratora interwale czasowym oraz status zasilania i chłodzenia aktywnego.

2.24. Gwarancja

- Dostawa musi zawierać również:
 - 24-miesięczną gwarancję producenta na dostarczone elementy systemu
 - Licencje na wszystkie funkcje bezpieczeństwa producentów ważne minimum do 30.06.2026 (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
 - Wsparcie techniczne świadczone przez Polskiego dystrybutora rozwiązań
 - Wdrożenie oferowanego rozwiązania przeprowadzone stacjonarnie na miejscu u Zamawiającego przez inżynierów posiadających Certyfikat poziomu profesjonalnego oferowanego rozwiązania (Zamawiający ma prawo wezwać Wykonawcę do okazania posiadanych Certyfikatów)
 - Oferta musi być złożona przez Autoryzowanego Partnera
 - Wykonawca musi posiadać doświadczenie we wdrażaniu technologii NGFW (Zamawiający ma prawo wezwać Wykonawcę do okazania referencji/potwierdzenia wdrożenia technologii NGFW).

Zadanie 12. System typu NGFW dla sieci IT HA

3. Przedmiot zamówienia

Przedmiotem dostawy są 1 sztuki urządzeń wraz z kompletem licencji niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego.

4. Wymagania dotyczące rozwiązania:

2.25. Elementy systemu bezpieczeństwa

- Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
- Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
- W zakresie Firewall, obsługa nie mniej niż 2 100 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
- Możliwość rozszerzenia pamięci do 1 TB poprzez dodatkowy dysk SSD
- Musi posiadać 1x USB 3.0 z przodu urządzenia
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
- System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji
- Systemy wirtualne muszą obsługiwać QOS
- System pełniący funkcję zapory musi posiadać nie mniej niż: 1x SFP+, 4x SFP, 4x GE interfejsów

2.26. Funkcjonalności

- Kontrola dostępu - zaporą sieciową Stateful Inspection
- Ochrona przed wirusami - komercyjny antywirus [AV]
- Poufność danych - IPSec VPN i SSL VPN
- Kontrola witryn sieci Web - filtr URL
- Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3)
- Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN
- Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
- Reputacja IP
- Cloud Sandbox

2.27. Wydajność

Wydajność dla 1 sztuki urządzenia:

- Analiza ruchu szyfrowanego protokołem SSL
- Wydajność Firewall co najmniej 2 Gb/s
- Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 1 Gb/s
- Wydajność w trybie NGFW Throughput (dla ruchu Enterprise Mix) minimum 2 Gbps
- Wydajność ochrony przed atakami (IPS) minimum 3Gb/s
- Wydajność AV nie mniej niż 2Gb/s
- Wydajność IPsec VPN, nie mniej niż 2 Gb/s

2.28. Funkcjonalności VPN

- Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
- Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
- Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności
- Praca w topologiach Hub and Spoke i Mesh
- Wspierane mechanizmy : IPsec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,
- Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24
- Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
- Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance)
- Obsługa PnPVPN (Plug and Play VPN)

2.29. Routing

- Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
- Obsługa Policy Based Routing
- Funkcjonalność Virtual Wire

2.30. Translacja adresów NAT

- Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
- Obsługa NAT46, NAT64, DNS64
- Wsparcie dla STUN

2.31. Polityka bezpieczeństwa systemu

- Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
- Możliwość budowania min. 11000 polityk
- Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
- Musi być w stanie skonfigurować agregowane polityki
- Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)

2.32. Wydzielenie stref bezpieczeństwa

- Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
- Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
- Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników

2.33. Ochrona antywirusowa

- Silnik antywirusowy musi być oparty na przepływie tzw. flow-based
- Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV
- Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB
- Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2,
- TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji

2.34. Równoważenie obciążenia

- Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
- Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin
- Kontrola stanu serwera, monitorowanie sesji i ochrona sesji

2.35. Ochrona IPS

- Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.
- Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
- Funkcjonalność zapobiegania atakom SQL injection, XSS injection
- Możliwość budowania własnych niestandardowych reguł IPS

2.36. Obrona przed atakiem

- Ochrona przed nieprawidłowym działaniem protokołu Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
- Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
- Biała lista docelowych adresów IP

2.37. Kontrola aplikacji

- Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP.
- Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka

2.38. Filtr adresów URL

- Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
- Możliwość zdefiniowania własnej bazy kategorii www.

- Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
- Kategorie takie jak hazard, malware, spam, botnety
- Obsługa Safe Search
- Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
- Dostosowanie strony ostrzeżenia

2.39. Ochrona danych

- Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
- Identyfikacja protokołu pliku, w tym HTTP, FTP, SMTP, POP3, IMAP
- Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
- Filtrowanie plików przesyłanych przez SMB

2.40. Reputacja IP

- Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force
- Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP

2.41. Zapobieganie botnetom

- Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
- Wsparcie DNS sinkhole
- Wsparcie wykrywania tunelowania DNS
- Wyrwanie i blokowanie DGA

2.42. Cloud Sandbox

- Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń
- Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
- Obsługa typów plików: PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
- Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń.

2.43. Uwierzytelnianie użytkownika

- System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu
- Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP
- Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazy danych
- Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
- Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory

- Wsparcie usług terminalowych
- Uwierzytelnianie użytkownika przez Web przed dostępem do internetu
- Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny

2.44. Raportowanie i przeglądanie logów

- Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
- W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
- Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego
- Generowanie co najmniej 10 rodzajów raportów

2.45. System logowania

- Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.

2.46. Certyfikaty

- Rozwiązanie musi:
 - posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
 - być pozycjonowanym w raporcie Gartnera nie dalej niż ostatnie 7 lat

2.47. Zarządzanie

- Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
- Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
- Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola
- W celu rozbudowy oraz integralności systemu bezpieczeństwa urządzenie musi pochodzić od tego samego producenta co SBDS, XDR, NIPS i umożliwiać zarządzanie wszystkimi urządzeniami z chmury producenta
- Urządzenie powinno monitorować i graficznie prezentować stan pracy urządzenia. Parametry takie jak obciążenie CPU oraz pamięć z podziałem na procesy, wykres zajętości dysku twardego w czasie, temperaturę urządzenia w wybranym przez administratora interwale czasowym oraz status zasilania i chłodzenia aktywnego.

2.48. Gwarancja

- Dostawa musi zawierać również:
 - 24-miesięczną gwarancję producenta na dostarczone elementy systemu
 - Licencje na wszystkie funkcje bezpieczeństwa producentów ważne minimum do 30.06.2026 (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
 - Wsparcie techniczne świadczone przez Polskiego dystrybutora rozwiązań
 - Wdrożenie oferowanego rozwiązania przeprowadzone stacjonarnie na miejscu u Zamawiającego przez inżynierów posiadających Certyfikat poziomu profesjonal

oferowanego rozwiązania (Zamawiający ma prawo wezwać Wykonawcę do okazania posiadanych Certyfikatów)

- Oferta musi być złożona przez Autoryzowanego Partnera

Wykonawca musi posiadać doświadczenie we wdrażaniu technologii NGFW (Zamawiający ma prawo wezwać Wykonawcę do okazania referencji/potwierdzenia wdrożenia technologii NGFW)

Zadanie 13. Usługi konfiguracji i hardeningu systemów/urządzeń IT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa profesjonalnej konfiguracji bezpieczeństwa (Hardening) oraz optymalizacji systemów informatycznych (IT). Celem jest zminimalizowanie powierzchni ataku (Attack Surface) oraz uszczelnienie komunikacji między siecią korporacyjną a infrastrukturą przemysłową

2. Wymagania dotyczące zakresu prac:

2.1. Hardening Systemowy (System-Level Hardening)

- Redukcja usług: Wyłączenie zbędnych protokołów, portów oraz usług systemowych niekrytycznych dla procesu technologicznego na serwerach.
- Zarządzanie dostępem: Konfiguracja rygorystycznych zasad haseł, uwierzytelniania wieloskładnikowego (MFA) oraz zasady minimalnych uprawnień (Least Privilege).
- Aktualizacje i Patche: Wdrożenie bezpiecznego procesu zarządzania poprawkami (Patch Management) z uwzględnieniem specyfiki systemów.

2.2. Bezpieczeństwo Sieciowe i Separacja (Network Hardening)

- Segmentacja IT: Fizyczna lub logiczna (VLAN, ACL) separacja sieci produkcyjnej od sieci biurowej zgodnie z normą IEC 62443.

2.3. Odporność Urządzeń (Device Hardening)

- Zabezpieczenie fizyczne: Blokada niewykorzystanych portów USB, napędów oraz interfejsów sprzętowych.
- Logowanie zdarzeń: Konfiguracja i optymalizacja systemów bezpieczeństwa ich zbierania logów w celu wykrywania włamań.

Zadanie 14. Stacja robocza fizyczna z rolą stacji przesiadkowej + dwa monitory 27 cali

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie 2 kompletów - komputera, instalacja oraz konfiguracja systemu typu Windows 11 pro, służącego do bezpiecznego, pośredniego dostępu zdalnego do urządzeń i stacji roboczych pracujących w sieci technologii operacyjnej (OT). System ma eliminować konieczność bezpośrednich połączeń z sieci biurowej do sieci OT.

2. Wymagania dotyczące rozwiązania

2.1. Minimalne wymaganie dla komputera

- Obudowa i konstrukcja Komputer w obudowie typu Small Form Factor (SFF)
- Jednostka centralna (Procesor) Procesor o architekturze minimum 14-tej generacji, posiadający co najmniej 4 rdzenie fizyczne. Taktowanie bazowe minimum 3.5 GHz, taktowanie w trybie Boost minimum 4.7 GHz. Pamięć podręczna L3 minimum 12 MB.
- Pamięć operacyjna RAM Zainstalowana pamięć RAM o pojemności minimum 16 GB, typu DDR5, o częstotliwości szyny minimum 4800 MHz. Płyta główna musi posiadać minimum 2 gniazda pamięci, z czego przynajmniej jedno musi pozostać wolne, umożliwiając rozbudowę do minimum 32 GB.
- Składowanie danych (Dysk) Dwa dysk twarde o pojemności minimum 480 GB, każdy
- Grafika i wideo Zintegrowany układ graficzny obsługujący minimum dwa monitory jednocześnie poprzez wbudowane złącza: minimum 1 x HDMI oraz minimum 1 x DisplayPort.
- Komunikacja i porty
 - LAN 2x10/100/1000 Mbit/s (RJ-45).
 - Złącza USB: minimum 1 x USB 3.2 Typ-C, 2 x USB 3.2 Typ-A oraz 4 x USB 2.0 Typ-A.
 - Złącze Audio typu Combo (słuchawki/mikrofon).
- Gniazda rozszerzeń i zasilanie
 - Płyta główna wyposażona w minimum: 1 x PCIe x16 oraz 2 x PCIe x1.
 - Zasilacz o mocy minimum 180 W, dostosowany do konfiguracji sprzętowej.
- System operacyjny i oprogramowanie
 - Zainstalowany system operacyjny Windows 11 Pro 64-bit w wersji polskiej
- Monitor
 - Proporcje obrazu 16:9
 - Przekątna ekranu 27"
 - Typ matrycy TFT IPS
 - Powierzchnia matrycy Matowa
- Akcesoria i gwarancja:
 - W zestawie przewodowa klawiatura (układ QWERTY PL).
 - Gwarancja minimum 3 lata

Zadanie 15. Usługa segmentacji sieci

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zaprojektowanie, konfiguracja oraz wdrożenie logicznej segmentacji sieci wewnątrzorganizacyjnej w celu zwiększenia poziomu bezpieczeństwa, optymalizacji ruchu sieciowego oraz odizolowania kluczowych zasobów IT.

2. Wymagania dotyczące zakresu prac

- 2.1.** Audyt i inwentaryzacja: Analiza obecnej topologii sieci, spisu urządzeń aktywnych (przełączniki, routery, firewalle) oraz identyfikacja typów ruchu sieciowego.
- 2.2.** Opracowanie projektu logicznego: Stworzenie schematu podziału na virtualne sieci lokalne (VLAN) wraz z adresacją IP dla każdego segmentu.
- 2.3.** Konfiguracja urządzeń sieciowych: Implementacja zaprojektowanych zmian na urządzeniach zamawiającego (konfiguracja portów access, trunk, tagowanie VLAN).
- 2.4.** Konfiguracja routingu i bezpieczeństwa: Uruchomienie routingu międzysegmentowego (Inter-VLAN Routing) oraz wdrożenie reguł filtrowania ruchu na zaporze sieciowej (Firewall/ACL).
- 2.5.** Testy i dokumentacja: Przeprowadzenie testów poprawności separacji oraz dostarczenie dokumentacji powykonawczej (schematy, tabele adresacji, opisy reguł firewall).
- 2.6.** Wykonawca zobowiązany jest do wydzielenia co najmniej następujących segmentów sieciowych (VLAN):
 - VLAN Administracja/Zarządzanie: Wyłącznie dla urządzeń sieciowych i serwerów (dostęp ograniczony).
 - VLAN Pracownicy: Dla stacji roboczych i laptopów służbowych.
 - VLAN Serwery: Dla zasobów udostępniających usługi (np. bazy danych, pliki).
 - VLAN IoT/Urządzenia biurowe: Dla drukarek, monitoringu, systemów kontroli dostępu.
 - VLAN Goście: Odizolowany segment z dostępem wyłącznie do Internetu, bez wglądu w sieć wewnętrzną.
 - VLAN VoIP: Priorytetyzowany ruch dla telefonii IP (QoS).
- 2.7.** Wymagania techniczne i standardy
 - Standardy: Praca w oparciu o protokół IEEE 802.1Q.
 - Bezpieczeństwo: Implementacja zasady "Zero Trust" – domyślne blokowanie ruchu między VLAN-ami, dopuszczanie tylko niezbędnych protokołów i portów.
 - WLAN: Integracja segmentacji z sieciami bezprzewodowymi (mapowanie SSID do odpowiednich VLAN).
- 2.8.** Harmonogram i warunki realizacji
 - Prace konfiguracyjne wpływające na ciągłość działania systemów muszą być prowadzone w oparciu o wcześniej ustalony plan okien serwisowych
- 2.9.** Dostarczona dokumentacja powykonawcza musi zawierać
 - Logiczny schemat sieci (np. w formacie PDF/Visio).

- Tabelę adresacji IP i przypisania VLAN.
- Matrycę przepływów (wykaz reguł Firewall/ACL).
- Instrukcję dla administratorów dotyczącą dodawania nowych urządzeń do odpowiednich segmentów.

Zadanie 16. Serwer do wykonywania kopii zapasowych (NAS)

1. Przedmiot zamówienia

Przedmiotem dostawy są 2 sztuki urządzeń serwerów plików typu NAS o pojemności (Surowa) nie mniejszej niż 14TB (ang. Raw Capacity) dla potrzeb kopii zapasowych wraz z zainstalowanym oprogramowaniem do zarządzania backupem i licencjami wieczystymi niezbędnymi do ich pełnego uruchomienia na wszystkich stacjach i serwerach zgodnie z poniższymi wymaganiami Zamawiającego.

2. Wymaganie dotyczące rozwiązania

- 2.1.** Konstrukcja i obudowa Serwer przeznaczony do montażu w szafie standardu 19 cali, o wysokości 1U. Obudowa o głębokości nieprzekraczającej 586 mm (bez panelu przedniego) oraz 599 mm (z panelem przednim typu Bezel). Urządzenie musi być wyposażone w panel bezpieczeństwa (bezel) zamykany na klucz lub opcjonalny filtr przeciwpyłowy.
- 2.2.** Procesor i płyta główna Serwer wyposażony w jeden procesor klasy x86, posiadający minimum 4 rdzenie fizycznych (np. z serii Intel Xeon E-2400 lub wydajniejszy).
- 2.3.** Pamięć operacyjna Minimum 16 GB DIMM pamięci DDR5 o taktowaniu minimum 4400 MT/s. Pamięć musi być wyposażona w mechanizm korekcji błędów (ECC UDIMM). Płyta główna musi umożliwiać rozbudowę pamięci RAM do co najmniej 128 GB.
- 2.4.** Kontrola składowania danych Serwer musi posiadać dedykowany, sprzętowy kontroler RAID montowany wewnątrz obudowy, wspierający dyski SAS/SATA/SSD. Dodatkowo wymagany jest niezależny podsystem startowy (Boot Optimized Storage Subsystem) obsługujący sprzętowy RAID dla dysku SSD.
- 2.5.** Zatoki dyskowe i pojemność Obudowa musi posiadać zatoki typu Hot-Swap dostępne od frontu urządzenia w jednej z poniższych konfiguracji:
 - Minimum 4 zatoki na dyski SAS/SATA (maksymalna pojemność min. 64 TB)
- 2.6.** Komunikacja sieciowa i złącza rozszerzeń Zintegrowana karta sieciowa 2 x 1 GbE (LOM). Serwer musi oferować minimum dwa wolne sloty rozszerzeń PCIe Gen4: jeden slot x8 (o szerokości pasma x8) oraz jeden slot x16 (o szerokości pasma x8), oba w formacie Low Profile/Half Length.
- 2.7.** Zasilanie i chłodzenie Pojedynczy zasilacz o mocy minimum 600W każdy, posiadający certyfikat sprawności energetycznej minimum Platinum (lub 700W Titanium). Chłodzenie realizowane za pomocą układu wentylatorów wewnętrznych (minimum 4 jednostki).

- 2.8.** Zarządzanie i bezpieczeństwo Zintegrowany kontroler zarządzania (BMC) posiadający dedykowany port sieciowy RJ-45 na tylnym panelu. Kontroler musi zapewniać dostęp przez interfejs WWW, wspierać standard Redfish API oraz umożliwiać zdalne blokowanie konfiguracji systemu (System Lockdown). Bezpieczeństwo musi być zapewnione przez moduł TPM 2.0 (FIPS, CC-TCG certified), mechanizm Secure Boot oraz funkcję Secure Erase do bezpiecznego usuwania danych z dysków.
- 2.9.** Interfejsy wejścia/wyjścia
- Front: 1 x USB 2.0, 1 x dedykowany port serwisowy (Micro-AB USB).
 - Tył: 1 x USB 2.0, 1 x USB 3.2 Gen1, 1 x VGA, 1 x Serial (RS-232).
 - Wewnątrz: 1 x USB 3.2 Gen1.
- 2.10.** Kompatybilność systemowa Pełne wsparcie producenta dla systemów operacyjnych: Microsoft Windows Server (z Hyper-V), Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Canonical Ubuntu Server LTS.
- 2.11.** Zarządzanie i magazyny
- Produkt dostępny w polskiej wersji językowej.
 - Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
 - System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
 - System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
 - System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
 - System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
 - System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
 - Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
 - System zarządzania nie może być oparty o relacyjne bazy danych.
 - Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
 - Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
 - Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
 - Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
 - System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykl.

- Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawcy (tzw. "no proprietary vendor lock").
- System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
- System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
- Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
- Rozwiązanie zapewnia backup jednorzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
- System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
- Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
- Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
- System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
- System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
- Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
- Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
- System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
- Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
- Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.

- Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
- System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
- Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
- Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
- Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
- Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
- Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
- Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
- Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
- System musi pozwalać na automatyczne aktualizacje oprogramowania.
- System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
- System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.
- System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmiennosć (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
- System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
- Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
- System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
- System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system

musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.

- Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
- W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
- Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
- System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
- System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,
- Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
- Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
- Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny
- Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
- Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
- Możliwość generowania raportów dobowych w oparciu o harmonogram
- Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)
- Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
- Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.

- Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

2.12. Wspierane systemy

- Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
 - Alpine 3.10+,
 - Debian: 9+,
 - Ubuntu: 16.04+,
 - Fedora: 29+,
 - CentOS: 7+,
 - RHEL: 6+,
 - openSUSE: 15+,
 - SUSE Enterprise Linux(SLES): 12 SP2+,
 - macOS: 10.13+,
 - Windows: 7, 8.1, 10(1607+),
 - Windows Server: 2008 R2+,
 - Środowisk wirtualnych:
 - Hyper-V 2016+,
 - VMware: 6.7+.
- Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
 - Debian: 9+
 - Ubuntu: 16.04+
 - Fedora: 29+
 - CentOS: 7+
 - RHEL: 6+
 - openSUSE: 15+
 - SUSE Enterprise Linux (SLES): 12 SP2+
 - Windows Client: 7, 8.1, 10 (1607+)
 - Windows Server: 2012 R2+,

2.13. Środowiska fizyczne i bazy danych

- Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
- Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
- Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
- Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.

- System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
- System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych.
- System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
- W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
- Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
- Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
- Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
- Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
- Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
- Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

2.14. Środowiska wirtualne

- System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
- System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
- System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
- Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.

- System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
- Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
- System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
- System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

2.15. Aplikacje SaaS

- Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
- Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
- System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
- System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
- System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
- System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
- System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
- System musi umożliwiać zabezpieczenie środowisk Jira
- System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.
- System musi umożliwiać zabezpieczenie środowisk Jira

2.16. Licencjonowanie i wsparcie techniczne

- Wszystkie linie supportu muszą być obsługiwane w języku polskim.
- Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
- Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
- Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
- Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
- Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.

- Licencje powinny być dostępne w opcji wieczystej .
- Dostęp do wsparcia technicznego producenta powinno obowiązywać przez minimum do 30.06.2026 r.
- Sposób licencjonowania opiera się na:
 - ilości serwerów/endpointów - dla fizycznych urządzeń,
 - ilości socketów w hostach - dla środowisk wirtualnych,
 - ilość repozytoriów - dla GIT.
- Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej minimum:
 - 16 stacji roboczych,
 - 2 serwerów

2.17. Anty-ransomware i bezpieczeństwo

- System plików rozwiązywania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
- System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
- System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
- W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
- System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.
- GWARANCJA minimum 5 lat.

Zadanie 17. System operacyjny na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie 1 sztuki licencji na serwerowy system operacyjny wspierający rozwiązanie do cyberbezpieczeństwa (lub najnowsza wersja dostępna w dniu składania ofert) w ilości pokrywającej zapotrzebowanie na wszystkie fizyczne rdzenie procesorów w serwerze.

2. Wymagania dotyczące rozwiązania

○ Wymagania ogólne:

2. Architektura: System musi być natywnie wspierany przez architekturę sprzętową posiadaną przez Zamawiającego (np. x86-64).
3. Wsparcie techniczne: Wykonawca musi dostarczyć system z prawem do bezpłatnych aktualizacji bezpieczeństwa i poprawek błędów przez okres minimum 3 lat.
4. Stabilność: System musi posiadać status wydania stabilnego (LTS Long Term Support lub równoważny).

○ Funkcjonalności sieciowe i domenowe

System musi zapewniać:

- Możliwość integracji z istniejącą usługą katalogową (np. Active Directory lub LDAP) w celu centralnego zarządzania użytkownikami i uprawnieniami.
- Wsparcie dla protokołów sieciowych: TCP/IPv4 oraz TCP/IPv6.
- Obsługę standardów współdzielenia plików i drukarek (np. SMB/CIFS, NFS).
- Możliwość zdalnej administracji systemem poprzez bezpieczne protokoły szyfrowane (np. RDP, SSH, HTTPS).

○ Bezpieczeństwo i zarządzanie

- Kontrola dostępu: System musi umożliwiać stosowanie polityk haseł, wieloskładnikowego uwierzytelniania (MFA) oraz zarządzania rolami (RBAC).
- Szyfrowanie: Wbudowany moduł do szyfrowania całych wolumenów dyskowych (standard AES lub równoważny).
- Audyt: Możliwość pełnego logowania zdarzeń systemowych, prób logowania oraz zmian w konfiguracji.
- Wirtualizacja: Wsparcie dla technologii konteneryzacji (np. Docker, Podman) oraz wirtualizacji (Hyper-V, KVM lub równoważne).

○ Interfejs i środowisko pracy

- Interfejs graficzny (GUI): System musi posiadać intuicyjny interfejs graficzny w języku polskim.
- Wiersz poleceń (CLI): Dostęp do zaawansowanego interpretera poleceń umożliwiającego automatyzację zadań (skryptowanie).
- Pakiet instalacyjny: System musi zawierać wbudowany menedżer pakietów/aplikacji do łatwej aktualizacji i instalacji oprogramowania.

Zadanie 18. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa pod system wirtualizacji (SIEM OT)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 sztuki serwera fizycznego niezbędnego do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa teleinformatycznego, stanowiącego platformę sprzętową dla systemu wirtualizacji wykorzystywanego na potrzeby środowiska SIEM OT. Oferowany serwer musi zapewniać parametry techniczne gwarantujące stabilne, wydajne i bezpieczne uruchomienie oraz eksploatację maszyn wirtualnych obsługujących funkcje zbierania, przetwarzania, korelacji i archiwizacji danych bezpieczeństwa pochodzących z infrastruktury OT.

2. Wymaganie dotyczące rozwiązania

- 2.1. Konstrukcja i obudowa Serwer przeznaczony do montażu w szafie standardu 19 cali, o wysokości 1U.
 - Obudowa o głębokości nieprzekraczającej 586 mm (bez panelu przedniego) oraz 599 mm (z panelem przednim typu Bezel).
 - Urządzenie musi być wyposażone w panel bezpieczeństwa (bezel) zamykany na klucz lub opcjonalny filtr przeciwpylowy.
- 2.2. Procesor i płyta główna
 - Serwer wyposażony w jeden procesor klasy x86, posiadający minimum 4 rdzeni fizycznych (np. z serii Intel Xeon E-2400 lub wydajniejszy).
- 2.3. Pamięć operacyjna Minimum 64 GB DIMM pamięci DDR5 o taktowaniu minimum 4400 MT/s.
 - Płyta główna musi umożliwiać rozbudowę pamięci RAM do co najmniej 128 GB.
- 2.4. Kontrola składowania danych
 - Serwer musi posiadać dedykowany, sprzętowy kontroler RAID montowany wewnątrz obudowy, wspierający dyski SAS/SATA/SSD.
 - Dodatkowo wymagany jest niezależny podsystem startowy (Boot Optimized Storage Subsystem) obsługujący sprzętowy RAID dla dysku SSD.
- 2.5. Zatoki dyskowe i pojemność
 - Obudowa musi posiadać zatoki typu Hot-Swap dostępne od frontu urządzenia w jednej z poniższych konfiguracji:
 - Minimum 2 dyski 480Gb SAS/SATA
 - Minimum 4 zatoki na dyski SAS/SATA (maksymalna pojemność min. 64 TB)
- 2.6. Komunikacja sieciowa i złącza rozszerzeń
 - Zintegrowana karta sieciowa 2 x 1 GbE (LOM).
 - Serwer musi oferować minimum dwa wolne sloty rozszerzeń PCIe Gen4: jeden slot x8 (o szerokości pasma x8) oraz jeden slot x16 (o szerokości pasma x8), oba w formacie Low Profile/Half Length.
- 2.7. Zasilanie i chłodzenie
 - Pojedynczy zasilacz o mocy minimum 600W każdy, posiadający certyfikat sprawności energetycznej minimum Platinum (lub 700W Titanium).

- Chłodzenie realizowane za pomocą układu wentylatorów wewnętrznych (minimum 4 jednostki).
- 2.8. Zarządzanie i bezpieczeństwo
 - Zintegrowany kontroler zarządzania (BMC) posiadający dedykowany port sieciowy RJ-45 na tylnym panelu.
 - Kontroler musi zapewniać dostęp przez interfejs WWW, wspierać standard Redfish API oraz umożliwiać zdalne blokowanie konfiguracji systemu (System Lockdown).
 - Bezpieczeństwo musi być zapewnione przez moduł TPM 2.0 (FIPS, CC-TCG certified), mechanizm Secure Boot oraz funkcję Secure Erase do bezpiecznego usuwania danych z dysków.
- 2.9. Interfejsy wejścia/wyjścia
 - Front: 1 x USB 2.0, 1 x dedykowany port serwisowy (Micro-AB USB).
 - Tył: 1 x USB 2.0, 1 x USB 3.2 Gen1, 1 x VGA, 1 x Serial (RS-232).
 - Wewnątrz: 1 x USB 3.2 Gen1.
- 2.10. Kompatybilność systemowa
 - Pełne wsparcie producenta dla systemów operacyjnych: Microsoft Windows Server (z Hyper-V), Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Canonical Ubuntu Server LTS
- 2.11. GWARANCJA- 5 lat.

Zadanie 19. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa pod rozwiązania bezpieczeństwa

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 sztuki serwera fizycznego niezbędnego do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa teleinformatycznego, przeznaczonego do obsługi systemu klasy PAM (Privileged Access Management). Oferowany serwer musi zapewniać parametry techniczne umożliwiające stabilną, wydajną i bezpieczną pracę rozwiązania służącego do zarządzania dostępem uprzywilejowanym, w tym obsługi sesji administracyjnych, rejestrowania aktywności, zarządzania politykami dostępu oraz bezpiecznego przechowywania poświadczeń.

2. Wymagania dotyczące rozwiązania

2.1. Konstrukcja i obudowa

- Serwer przeznaczony do montażu w szafie standardu 19 cali, o wysokości 1U.
- Obudowa o głębokości nieprzekraczającej 586 mm (bez panelu przedniego) oraz 599 mm (z panelem przednim typu Bezel).

- Urządzenie musi być wyposażone w panel bezpieczeństwa (bezel) zamykany na klucz lub opcjonalny filtr przeciwpyłowy.
- 2.2.** Procesor i płyta główna
 - Serwer wyposażony w jeden procesor klasy x86, posiadający minimum 4 rdzeni fizycznych (np. z serii Intel Xeon E-2400 lub wydajniejszy).
- 2.3.** Pamięć operacyjna
 - Minimum 16 GB DIMM pamięci DDR5
 - Płyta główna musi umożliwiać rozbudowę pamięci RAM do co najmniej 128 GB.
- 2.4.** Kontrola składowania danych
 - Serwer musi posiadać dedykowany, sprzętowy kontroler RAID montowany wewnątrz obudowy, wspierający dyski SAS/SATA/SSD.
 - Dodatkowo wymagany jest niezależny podsystem startowy (Boot Optimized Storage Subsystem) obsługujący sprzętowy RAID dla dysku SSD.
- 2.5.** Zatoki dyskowe i pojemność
 - Obudowa musi posiadać zatoki typu Hot-Swap dostępne od frontu urządzenia w jednej z poniższych konfiguracji:
 - Minimum 1 dyski 480 Gb SAS/SATA
 - Minimum 4 zatoki na dyski SAS/SATA (maksymalna pojemność min. 64 TB)
- 2.6.** Komunikacja sieciowa i złącza rozszerzeń
 - Zintegrowana karta sieciowa 2 x 1 GbE (LOM).
 - Serwer musi oferować minimum dwa wolne sloty rozszerzeń PCIe Gen4: jeden slot x8 (o szerokości pasma x8) oraz jeden slot x16 (o szerokości pasma x8), oba w formacie Low Profile/Half Length.
- 2.7.** Zasilanie i chłodzenie
 - Pojedynczy zasilacz o mocy minimum 600W każdy, posiadający certyfikat sprawności energetycznej minimum Platinum (lub 700W Titanium).
 - Chłodzenie realizowane za pomocą układu wentylatorów wewnętrznych (minimum 4 jednostki).
- 2.8.** Zarządzanie i bezpieczeństwo
 - Zintegrowany kontroler zarządzania (BMC) posiadający dedykowany port sieciowy RJ-45 na tylnym panelu.
 - Kontroler musi zapewniać dostęp przez interfejs WWW, wspierać standard Redfish API oraz umożliwiać zdalne blokowanie konfiguracji systemu (System Lockdown).
 - Bezpieczeństwo musi być zapewnione przez moduł TPM 2.0 (FIPS, CC-TCG certified), mechanizm Secure Boot oraz funkcję Secure Erase do bezpiecznego usuwania danych z dysków.
- 2.9.** Interfejsy wejścia/wyjścia
 - Front: 1 x USB 2.0, 1 x dedykowany port serwisowy (Micro-AB USB).
 - Tył: 1 x USB 2.0, 1 x USB 3.2 Gen1, 1 x VGA, 1 x Serial (RS-232).
 - Wewnątrz: 1 x USB 3.2 Gen1.
- 2.10.** Kompatybilność systemowa

- Pełne wsparcie producenta dla systemów operacyjnych: Microsoft Windows Server (z Hyper-V), Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Canonical Ubuntu Server LTS

2.11. Gwarancja - 5 lat.

Zadanie 20. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 sztuki szafy teleinformatycznej w standardzie rack 42U.

2. Wymaganie dotyczące rozwiązania

Szafa serwerowa stojąca o wysokości 42U, przeznaczona do instalacji urządzeń sieciowych, serwerowych oraz telekomunikacyjnych w standardzie 19" - 1 szt.

- Cechy i wyposażenie:
 - Szafa przeznaczona do samodzielnego montażu (FLAT PACK)
 - Przepusty kablowe od góry i od dołu
 - Drzwi przednie i tylne perforowane
 - Klasa szczelności: IP20
 - Maksymalne statyczne obciążenie: 1200 kg
 - Panel LCD do monitoringu parametrów temperatury i wentylatorów
 - Termostat oraz panel wentylacyjny z 6 wentylatorami w zestawie
 - Szafa wyposażona w zamek przedni, tylny oraz zamki boczne
- Parametry techniczne:
 - Rodzaj szafy: stojąca
 - Rozmiar: 19"
 - Wysokość teleinformatyczna: 42U
 - Szerokość: 800 mm
 - Głębokość całkowita: 1000 mm
 - Głębokość montażowa: 860 mm
 - Klasa szczelności IP20
- Wyposażenie dodatkowe:
 - 1 patchpanel 6cat 48 gniazd
 - 4 Organizery kabli
 - Gniazda na zaślepki na 20 U
 - 2 listwy zasilające poziome
 - 20 patcordów 100cm światłowodowych S.C.
 - 50 patcordów 25cm

- 50 patcordów 50cm

50 patcordów 100cm

Zadanie 21. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuk zarządzalnych urządzeń sieciowych, umożliwiających segmentację ruchu z wykorzystaniem VLAN, zabezpieczenie transmisji danych z zastosowaniem technologii MACsec zgodnych z wymaganiami technicznymi określonymi w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania

2.1. Szczegółowa specyfikacja techniczna

Cecha	Wymagania minimalne
Typ urządzenia	Przełącznik zarządzalny L2/L3, typ Desktop (bezwentylatorowy)
Liczba portów	8 portów RJ-45 Gigabit Ethernet (10/100/1000 Mbps)
Wydajność przełączania	Minimum 16 Gbps
Szybkość przekierowań	Minimum 11.9 Mpps
Pamięć	RAM: 2 GB; Flash: 1 GB

Standardy sieciowe	IEEE 802.3, 802.3u, 802.3ab, 802.3z, 802.3ad (LACP), 802.1Q (VLAN), 802.1p (CoS), 802.1x, 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP)
Zarządzanie	Interfejs webowy (GUI), CLI (Telnet/SSH), SNMP v1/v2c/v3, Cisco Business Mobile App, wsparcie dla Cisco Business Dashboard
Bezpieczeństwo	Listy kontroli dostępu (ACL), Port Security, IEEE 802.1X, ochrona przed atakami DoS, DHCP Snooping
Funkcje Layer 3	Routing statyczny IPv4/IPv6 (do 32 tras), routing między VLAN-ami
Kolor obudowy	Biały

2.2. Wymagania dodatkowe:

- Chłodzenie: Pasywne, co zapewnia bezgłośną pracę urządzenia.
- Zasilanie: Zewnętrzny zasilacz sieciowy dołączony do zestawu.
- Gwarancja: Minimum 24 miesiące gwarancji producenta
- Stan produktu: Urządzenie musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek europejski, być fabrycznie nowe i nieużywane.

Zadanie 22. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuk punktu dostępowego sieci bezprzewodowej WiFi, przystosowanych do zasilania w standardzie PoE, spełniających wymagania techniczne i funkcjonalności określone przez Zamawiającego

2. Wymaganie dotyczące rozwiązania

2.1. Standardy bezprzewodowe i wydajność:

- Obsługiwane standardy: IEEE 802.11a/b/g/n/ac (Wave 2) oraz 802.11ax (Wi-Fi 6).
- Tryb pracy: Dual-band, jednoczesna obsługa pasm 2,4 GHz oraz 5 GHz.

- Maksymalna przepustowość: Minimum 1,2 Gbps w paśmie 5 GHz.
- Obsługa technologii: MU-MIMO (minimum 2x2), OFDMA, TWT (Target Wake Time).
- Pojemność sieci: * Minimum 200 klientów bezprzewodowych na jedno radio.
 - Łączna obsługa minimum 400 klientów bezprzewodowych na urządzenie.

2.2. Specyfikacja sprzętowa:

- Procesor: Taktowanie minimum 1 GHz.
- Pamięć RAM: Minimum 1 GB.
- Pamięć Flash: Minimum 512 MB.
- Interfejsy przewodowe: Minimum 1 port RJ-45 10/100/1000 Mbps (Gigabit Ethernet).
- Anteny: Zintegrowane (wewnętrzne) o charakterystyce dookólnej.
- Zasilanie: Obsługa standardu Power over Ethernet (PoE) zgodnie z IEEE 802.3af/at.

2.3. Funkcjonalności i zarządzanie:

- Zarządzanie: Możliwość konfiguracji i monitorowania poprzez dedykowaną aplikację mobilną oraz interfejs WWW (Web UI).
- Obsługa VLAN: Wsparcie dla minimum 16 sieci VLAN (segmentacja ruchu).
- Bezpieczeństwo: Obsługa protokołów WPA2, WPA3, filtrowanie adresów MAC, izolacja klientów.
- Funkcje dodatkowe: Wsparcie dla sieci typu Mesh (możliwość bezprzewodowego łączenia punktów dostępowych).
- Montaż: W komplecie zestaw do montażu sufitowego lub ściennego.

Zadanie 23. Oprogramowanie typu ITSM (Information Technology Service Management)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 30 sztuki licencji oprogramowania typu ITSM wraz z kompletem licencji ważnych minimum do 30.06.2026 r. niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego.

2. Wymaganie dotyczące rozwiązania

2.1. Specyfikacja Techniczna

- Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.
- Konsola web administratora musi posiadać możliwość wyboru języka polskiego.
- Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.
- Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi i odrębnie między urządzeniami mobilnymi

- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.
- Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.
- Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.
- Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.
- Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.
- Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.
- Konsola web umożliwia zmianę ustawień priorytetu skanowania.
- Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.
- Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.
- Konsola web musi umożliwiać synchronizację z Azure Active Directory.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z stacji klienckiej.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.
- Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.
- Konsola web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta oraz przez użytkownika w języku Python lub JSON.

2.2. Zarządzanie aktualizacjami

- Oprogramowanie web musi zawierać zintegrowaną funkcjonalność menadżera aktualizacji (Patch Manager), który umożliwia zarządzanie pobieraniem aktualizacji (update'ów) systemu Windows, Java, Adobe i innych producentów trzecich.
- Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 50 producentów.

2.3. Zarządzanie użytkownikami i stacjami

- Rozwiązanie musi umożliwiać bezpośrednio z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich o minimalnych, następujących funkcjonalnościach:

- Czyszczenie plików tymczasowych
 - Czyszczenie i sprawdzanie dysku
 - Usuwanie błędów dysku
 - Defragmentowanie dysku
 - Czyszczenie kolejki drukarki
 - Czyszczenie pamięci podręcznej DNS
 - Czyszczenie kosza
 - Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check
 - Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows
- System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu.
 - System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit.
 - Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows.
 - Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkownika przez administratora w określonym przez niego czasie.
 - Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkownika przez administratora w celu odpytania go o zgodę na połączenie.
 - Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli.
 - Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

Zadanie 24. Oprogramowanie typu MDM (Mobile Device Management)

3. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuki licencji oprogramowania MDM wraz z kompletem licencji niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego. Subskrypcja licencji ważna minimum do 30.06.2026 r.

4. Wymaganie dotyczące rozwiązania

2.1. Specyfikacja Techniczna

- Konsola web administratora powinna znajdować się w chmurze producenta
- znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.
- Konsola web administratora musi posiadać możliwość wyboru języka polskiego.

- Konsola web musi umożliwiać zarządzanie urządzeniami mobilnymi poprzez tę samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla urządzeń mobilnych.
- Administrator musi mieć możliwość przeniesienia z poziomu konsoli aktywnej licencji na inne urządzenie mobilne bez utraty ważności licencji.
- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.
- Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na urządzeniach mobilnych.
- Konsola web musi umożliwiać geolokalizację z aktualną mapą urządzeń mobilnych iOS/Android wyposażonych w moduł GPS.
- Konsola web musi mieć możliwość zdefiniowania zalecanych aplikacji, które może pobrać użytkownik urządzeń mobilnych.
- Konsola web umożliwia zdalną deinstalację jak i blokadę aplikacji firm trzecich na urządzeniu mobilnym
- Konsola web musi umożliwiać wyczyszczenie lub zablokowanie zdalne urządzenia mobilnego.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla urządzeń mobilnych
- Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z urządzenia mobilnego.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.
- Konsola web musi mieć funkcję tworzenia raportów o urządzeniach mobilnych w konsoli.
- Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

2.2. Konsola i oprogramowanie umożliwia :

- Włączenie/Wyłączenie syreny na urządzeniu mobilnym
- Wysłanie komunikatu do urządzenia mobilnego
- Zmianę kodu dostępu
- Blokowanie/Odblokowanie aplikacji oraz ich deinstalację
- Zdjęcie z przedniej kamery w przypadku przekroczenia ilości prób logowania
- Aktualizacja lokalizacji urządzenia mobilnego
- Całkowite wyczyszczenia urządzenia
- Blokada urządzenia
- Zmiana hasła dostępu

- Wspiera funkcję ActiveSync
- Użyj szyfrowania serwera poczty przychodzącej (SSL)
- Akceptuj wszystkie certyfikaty (dla poczty przychodzącej)
- Zaakceptuj certyfikaty TLS (dla poczty przychodzącej)
- korzystanie z certyfikatu
- Zabroń przemieszczania poczty na inne konta
- Tryb Kiosk dla urządzeń
- Konfigurację VPN (L2TP/PPTP/L2TP IPSEC PSK/IPSEC XAUTH PSK/IPSEC XAUTH RSA)
- Oprogramowanie umożliwia ograniczenia korzystania z Bluetooth
- Zezwalaj/Zablokuj na wykrywanie urządzeń przez Bluetooth
- Pozwól/Zablokuj na parowanie urządzenia Bluetooth
- Zezwalaj/Zablokuj na połączenia wychodzące
- Zezwól/Zablokuj na Tethering przez Bluetooth
- Zezwalaj/Zablokuj na połączenie z komputerem stacjonarnym lub laptopem przez Bluetooth
- Zezwalaj/Zablokuj na przesyłanie danych
- Oprogramowanie umożliwia ograniczenia korzystania z przeglądarki
- Zezwalaj/Zablokuj na wyskakujące okienka
- Pozwól/Zablokuj korzystać z JavaScript
- Akceptuje/Zablokuj ciasteczka
- Zapamiętaj/Zablokuj dane formularza do późniejszego wykorzystania
- Pokaż/Zablokuj ustawienia ostrzeżeń o oszustwach
- Oprogramowanie umożliwia ograniczenia korzystania z aplikacji
- Zezwól/Zablokuj na korzystanie z Gmaila
- Zezwól/Zablokuj na korzystanie z poczty e-mail
- Zezwól/Zablokuj na korzystanie z przeglądarki
- Zezwól/Zablokuj na korzystanie z galerii
- Zezwól/Zablokuj na Google Play
- Zezwól/Zablokuj na korzystanie z aplikacji YouTube
- Zezwól/Zablokuj na Mapy Google i nawigację Google
- Zezwól/Zablokuj na wyszukiwanie Google i głosowe
- Zezwól/Zablokuj Chrome Browser
- Zezwól/Zablokuj Galaxy Store

2.3. Oprogramowanie ogranicza:

- Zezwól/Zablokuj na połączenie z USB
- Zezwól/Zablokuj użyj czasu sieciowego
- Zezwól/Zablokuj korzystać z mikrofonu
- Zezwól/Zablokuj na Near Field Communication (NFC)
- Zezwól/Zablokuj na fałszywe lokalizacje

- Zezwól/Zablokuj na dostęp do karty SD
- Zezwól/Zablokuj na zapis na karcie SD
- Zezwól/Zablokuj na przechwytywanie ekranu
- Zezwól/Zablokuj na korzystanie ze schowka
- Zezwól/Zablokuj utworzenie kopii zapasowej moich danych
- Zezwól/Zablokuj widoczne hasła
- Zezwól/Zablokuj na debugowanie USB
- Zezwól/Zablokuj na reset fabryczny
- Zezwól/Zablokuj na aktualizację OTA

2.4. Platforma powinna mieć obsługę w języku polskim.

2.5. Platforma powinna obsługiwać systemy operacyjne:

- **Android**
 - 9.x
 - 9.x(KNOX)
 - 10.x
 - 10.x(KNOX)
 - 11.x
 - 11.x(KNOX)
 - 12.x
 - 12.x(KNOX)
 - 13.x
 - 13.x (KNOX)
 - 14.x
 - 14.x(KNOX)
 - 15.x
 - 15.x (KNOX)
- **iOS**
 - 15.x
 - 16.x
 - 17.x
 - 18.x
 - 19.x
 - 26.x

Zadanie 25. Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 30 sztuk licencji oprogramowania DLP wraz z kompletem licencji na niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego. Subskrypcja licencji ważna minimum do 30.06.2026 r.

2. Wymaganie dotyczące rozwiązania

2.1. Konsola zarządzająca

- Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.
- Konsola web administratora musi posiadać możliwość wyboru obsługi interfejsu w języku polskim.
- Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.
- Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi.
- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.
- Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.
- Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.
- Konsola web umożliwia zmianę ustawień priorytetu skanowania.
- Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.
- Konsola web musi umożliwiać synchronizację z Azure Active Directory.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z aplikacji zainstalowanej na stacji klienckiej.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych.
- Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.
- Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli.
- Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

2.2. Platforma powinna obsługiwać systemy operacyjne:

- mac OS:
 - 10.14.x
 - 10.15.x
 - 11.x
 - 12.x
 - 13.x
 - 14.x
 - 15.x
- MS Windows (stacje klienckie):
 - Windows XP (SP3 or higher) x86
 - Windows 7 SP1 x86
 - Windows 7 SP1 x64
 - Windows 8 x86
 - Windows 8 x64
 - Windows 8.1 x86
 - Windows 8.1 x64
 - Windows 10 x86
 - Windows 10 x64
 - Windows 11 x64
- MS Windows (wersja serwerowa):
 - Windows Server 2003 SP2
 - Windows Server 2003 R2 SP2
 - Windows Server 2008 SP2
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
 - Windows Server 2025
- LinuxOS z gwarantowaną kompatybilnością:
 - Latest Ubuntu 16.x LTS x64 release version (with GUI)
 - Latest Ubuntu 18.x LTS x64 release version (with GUI)
 - Latest Ubuntu 19.x x64 release version (with GUI)
 - Latest Ubuntu 20.x LTS x64 release version (with GUI)
 - Latest Ubuntu 21.04 x64 release version (with GUI)
 - Latest Ubuntu 22.04 x64 release version (with GUI)
 - Latest Debian 8.x x64 release version (with GUI)
 - Latest Debian 9.x x64 release version (with GUI)
 - Latest Debian 10.x x64 release version (with GUI)
 - Latest Red Hat Enterprise Linux Server 7.x x64 release version (with GUI)
 - Latest Red Hat Enterprise Linux Server 8.x x64 release version (with GUI)

- Latest CentOS 7.x x64 release version (with GUI)
- Latest CentOS 8.x x64 release version (with GUI)

2.3. Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:

- 512 MB dostępnej pamięci RAM
- 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej
- Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI

2.4. Funkcjonalność

- Konsola web musi posiadać moduł zapobiegania wyciekowi danych DLP z możliwością włączenia skanowania plików w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna umożliwiać sprawdzenia logów z tej czynności.
- System musi umożliwiać wyszukiwanie i ochronę plików w oparciu o wybrane kryteria w tym między innymi: numer PESEL, numer dowodu osobistego, numer paszportu, numer karty bankowej, numer IBAN, określone ciągi znaków oraz wybrane wyrażenia.
- Program DLP musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji.
- Program DLP musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB
- Program DLP musi posiadać moduł ochrony przed wyciekiem działający w czasie rzeczywistym.
- Program DLP musi posiadać moduł sprawdzający reputację plików w chmurze.
- Podczas pracy komputera Program musi automatycznie skanować:
 - pliki uruchamiane, otwierane,
 - pliki kopiowane lub przenoszone,
 - pliki tworzone,
 - pliki pobierane z Internetu po protokole HTTP/HTTPS.
- Program powinien posiadać zintegrowaną funkcję skanowania i ochrony plików pod kątem danych wrażliwych (DLP).
- Program powinien chronić przed nieupoważnionym zrzutem obrazu z ekranu.
- Program umożliwia na rejestrowanie dzienników zdarzeń oraz zapisywanie ich lokalnie i na zewnętrznym serwerze.
- Program umożliwia tworzenie i analizowanie raportów dotyczących pracy systemu oraz wykrytych naruszeń.

Zadanie 26. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usługi zarządzanego wykrywania i reagowania (MDR) w modelu 8/5 (dni robocze, godz. 8:00 – 16:00) realizowane minimum do 30.06.2026. Usługa obejmuje wsparcie ekspertów w wymiarze 200 roboczogodzin (h).

2. Wymagania dotyczące usługi

- 2.1. Wykonawca zobowiązany jest do cyklicznego wg ustalonego harmonogramu monitorowania, zarządzania oraz analizy zdarzeń z następujących komponentów infrastruktury Zamawiającego:
- Network (Sieć): Zarządzanie i monitoring przełączników (Switches).
 - Brzeg sieci (NGFW): Administracja i analiza logów z zapór ogniowych nowej generacji.
 - Analiza ruchu (NDR): Monitorowanie anomalii w ruchu sieciowym (Network Detection and Response).
 - Decepcja (HoneyPot): Utrzymanie i analiza incydentów z pułapek typu HoneyPot.
 - Endpoint Protection: Ochrona antymalware/EDR na stacjach roboczych (PC) oraz serwerach.
- 2.2. Zakres obowiązków Wykonawcy
- Analiza zdarzeń krytycznych: Wykonawca jest zobowiązany do priorytetowej analizy wyłącznie incydentów zakwalifikowanych jako Krytyczne (Critical/High).
 - Raportowanie zewnętrzne: W przypadku potwierdzenia incydentu o charakterze naruszenia bezpieczeństwa, Wykonawca powinien przygotować zgłoszenie incydentu do właściwego zespołu CSIRT/CERT (zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa).
 - Zarządzanie zmianą: Konfiguracja i optymalizacja ww. systemów w ramach dostępnej puli godzin.
- 2.3. Wykonawca musi wykazać, że posiada zasoby i doświadczenie gwarantujące należyłą jakość usługi:
- Certyfikacja Organizacyjna: Wykonawca lub podmiot świadczący usługi musi posiadać aktualny certyfikat ISO/IEC 27001 (System Zarządzania Bezpieczeństwem Informacji).
 - Potencjał Kadrowy: Wykonawca skieruje do realizacji zamówienia co najmniej 2 inżynierów, z których każdy posiada:
 - Certyfikat poziomu Professional (lub równoważny) wydany przez producentów rozwiązań dostarczonych w ramach postępowania (np. certyfikaty z zakresu NGFW, NDR lub Endpoint Protection).
 - Minimum 5-letnie udokumentowane doświadczenie w pracy z oferowanymi rozwiązaniami cyberbezpieczeństwa w w/w postępowaniu.
- 2.4. Parametry SLA i komunikacja

Parametr	Wymaganie
Dostępność usługi	Dni robocze, 08:00 – 16:00.

Czas reakcji na incydent krytyczny	Czas Podjęcia zgłoszenia (Response Time) do 6h od wykrycia zdarzenia w godzinach pracy.
Kanał zgłoszeniowy	System ticketowy oraz dedykowany adres e-mail, telefon.
Raportowanie	Cykliczne raportowanie o incydentach

Zadanie 27. Oprogramowanie do zarządzania tożsamością i dostępem w trybie brokera sesji

1. Przedmiot zamówienia

Przedmiotem dostawy jest dostarczenie 10 sztuk licencji oprogramowania do zarządzania tożsamością i dostępem wraz z kompletem licencji na niezbędnych do ich pełnego uruchomienia i eksploatacji zgodnie z poniższymi wymaganiami Zamawiającego. Licencje bezterminowe lub ważne minimum do 30.06.2026 r.

2. Wymagania dotyczące oprogramowania

2.1. Wymagania Funkcjonalne

- Obsługa Protokołów: Pełne wsparcie dla protokołów RDP, VNC, SSH
- Dostęp przez Przeglądarkę: Całość interfejsu użytkownika i sesji zdalnych musi być realizowana wewnątrz przeglądarki (obsługa standardu HTML5).
- Zarządzanie Połączeniami: Możliwość definiowania wielu połączeń dla różnych grup użytkowników z parametrami takimi jak: rozdzielczość, głębokość kolorów, mapowanie dysków i drukarek (dla RDP).
- Transfer Plików: Możliwość przesyłania plików między urządzeniem lokalnym a zdalnym (jeśli protokół na to pozwala) za pośrednictwem interfejsu przeglądarki.
- Wsparcie dla Clipboard: Obsługa kopiowania i wklejania tekstu pomiędzy systemem lokalnym a zdalnym.
- Nagrywanie Sesji: Możliwość rejestracji sesji graficznych (RDP/VNC) oraz tekstowych (SSH) do celów audytowych w formacie umożliwiającym późniejsze odtworzenie.

2.2. Bezpieczeństwo i Autoryzacja

- Integracja z Katalogiem: Możliwość autoryzacji użytkowników poprzez Active Directory (LDAP/S) lub protokoły SAML / OpenID Connect.
- Szyfrowanie: Cała komunikacja między użytkownikiem a bramą musi odbywać się przez szyfrowany protokół HTTPS (TLS 1.2/1.3) z wykorzystaniem certyfikatów zaufanego urzędu certyfikacji.

- Izolacja Sieciowa: System musi działać jako pośrednik (proxy), nie wymagając bezpośredniego routingu między urządzeniem użytkownika a docelowym serwerem wewnętrznym.

2.3. Wymagania Techniczne (Wdrożenie)

- Konteneryzacja: (Opcjonalnie) Preferowane wdrożenie w oparciu o architekturę kontenerową (np. Docker Compose / Kubernetes) w celu łatwego skalowania i aktualizacji.
- Baza Danych: Wykorzystanie relacyjnej bazy danych (PostgreSQL lub MySQL) do przechowywania konfiguracji, uprawnień i historii logowań.
- Wydajność: System musi obsługiwać do 3 jednoczesnych sesji zdalnych bez zauważalnych opóźnień (tzw. *lagów*) przy założeniu standardowej pracy biurowej.

Zadanie 28. Oprogramowanie lub urządzenie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 32 sztuk rozwiązania typu MFA (Multi-Factor Authentication) w postaci oprogramowania lub urządzenia wyposażonego w czytnik linii papilarnych, przeznaczonego do realizacji wieloskładnikowego uwierzytelniania użytkowników, zgodnego z wymaganiami technicznymi i funkcjonalnymi określonymi przez Zamawiającego.

2. Wymagania dotyczące rozwiązania:

2.1. Wymagania techniczne:

- Sensor biometryczny: Zintegrowany z obudową myszy, pojemnościowy czytnik linii papilarnych.
- Bezpieczeństwo danych: Szyfrowanie wzorca linii papilarnych na poziomie sprzętowym (np. technologia *Match-in-sensor*).
- Standardy łączności: Przewodowa (USB) lub bezprzewodowa z odbiornikiem zapewniającym bezpieczną transmisję danych.
- Ergonomia: Konstrukcja pełnowymiarowa, min. 3 przyciski + rolka przewijania, rozdzielczość sensora optycznego min. 1000 DPI.

2.2. Wymagania dotyczące kompatybilności (Kluczowe) aby urządzenie mogło pełnić rolę drugiego składnika (MFA) w , musi spełniać poniższe normy:

- Wsparcie FIDO2 / WebAuthn: Urządzenie musi być rozpoznawane przez system operacyjny i przeglądarkę internetową (Chrome/Edge/Firefox) jako klucz bezpieczeństwa zgodny ze standardem FIDO2.

- Certyfikacja Windows Hello: Pełna zgodność z mechanizmem Windows Hello w systemach Windows 10/11 (umożliwiająca logowanie biometryczne do systemu operacyjnego).
- Standard Plug & Play: Praca bez konieczności instalacji niestandardowych sterowników firm trzecich, które mogłyby naruszać politykę bezpieczeństwa stacji roboczej.

Zadanie 29. Klucze sprzętowe U2F

1. Przedmiot dostawy

Przedmiotem zamówienia jest dostawa 1 sztuki sprzętowego tokena uwierzytelniającego standard U2F/FIDO2, wyposażonych w interfejs USB-A oraz obsługę komunikacji NFC, kompatybilnych z rozwiązaniami klasy MFA, spełniających wymagania techniczne określone w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania:

2.1. Opis techniczny:

- Rozwiązanie sprzętowe skutecznie chroniące m.in. przed phishingiem.
- Posiada wsparcie dla platform: Microsoft Windows, Mac OS, Linux, Chrome OS.
- Umożliwia współpracę z mobilnymi systemami operacyjnymi iOS oraz Android.
- Jest kompatybilny z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox.
- Jest kompatybilny z serwisami: Google, Microsoft, Twitter, Facebook, Instagram, Gmail, Google Drive i YouTube.
- Posiada możliwość potwierdzenia logowania dotknięciem przycisku - obowiązkowa interakcja użytkownika podczas logowania.
- Posiada wsparcie dla PKCS#11.
- Obsługuje algorytmy kryptograficzne: RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384.
- Jest odporny na zgniecenie.
- Posiada klasę szczelności IP68.
- Nie wymaga baterii.
- Nie wymaga połączenia internetowego.
- Nie jest typem pendrive, czyli nie posiada miejsca do przechowywania danych: pliki, katalogi.
- Nie działa po Bluetooth.
- Posiada możliwość wygrawerowania loga/kodu.
- Jest tak fizycznie skonstruowany, by uniemożliwić jego rozłożenie na części i ponowne złożenie.
- Nie obsługuje logowania za pomocą biometrii.
- Umożliwia przechowywanie na nim kodów OTP, zamiast np. w aplikacji mobilnej.
- Posiada specjalne oczko umożliwiające zawieszenie urządzenia.

- Klucz sprzętowy do dwupoziomowego uwierzytelnienia, który posiada certyfikację U2F i FIDO2.
- Klucz jest produkowany tylko w EU lub USA.
- Posiada NFC, by można było zdalnie przekazać kod do urządzenia mobilnego.
- Złącze na USB A.
- Klucz jest zasilany tylko z portu USB lub wyzwala tag NFC po przyłożeniu do urządzenia mobilnego.
- Klucz wyzwala tag NFC (kod FIDO/FIDO2 w aplikacji mobilnej) po przyłożeniu do urządzenia mobilnego.
- Klucz jest tak zabezpieczony przez producenta, że nie ma możliwości wykonania jego kopii na inny klucz czy też dokonania manipulacji w obrębie jego oprogramowania.
- Oprogramowanie do zarządzania kluczem jest udostępnione do pobrania ze strony producenta.
- Klucz sprzętowy posiada oprócz U2F i FIDO2 również inne możliwości logowania czy obsługi szyfrowania, jak: smart card, Open PGP, OTP, kody zdarzeniowe i czasowe TOTP/HOTP, statyczne hasło oraz Challenge-Response.
- Klucz posiada możliwość zaprogramowania dwóch dodatkowych portów o dodatkowe funkcje:
 - OTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą darmowej aplikacji producenta)
 - kody zdarzeniowe i czasowe TOTP/HOTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą darmowej aplikacji producenta)
 - statyczne hasło
 - Challenge-Response
- Dostępność oprogramowania/bibliotek/API na stronie producenta na zasadzie open source, w celu integracji z niestandardowymi aplikacjami.

Zadanie 30. Usługa inwentaryzacji aktywów teleinformatycznych IT.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usługi inwentaryzacji aktywów teleinformatycznych w obszarach IT. Celem realizacji usługi jest przeprowadzenie analizy istniejącej dokumentacji oraz instalacji obiektowych, w celu opracowania materiałów i produktów wstępnych niezbędnych do rozpoczęcia pierwszych etapów projektowania.

2. Wymagania dotyczące usługi

2.1. Zakres ogólny

- Wprowadzenie i wstępne spotkanie robocze

- Cel: Uzyskanie wspólnej wizji realizacji prac fazy wraz z ustaleniem wytycznych i zakresu merytorycznego prac. Przekazanie dokumentacji. Omówienie dokumentacji i jej zakresu merytorycznego.
- Przygotowanie produktów wstępnych procesu inwentaryzacji (karty inwentaryzacji)
- Miejsce realizacji prac fazy
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY

2.2. Inwentaryzacja obiektów fizycznych w formie Audytu - Zakres ogólny

- Wprowadzenie i wstępne spotkanie robocze
 - Cel: Ustalenie wytycznych i zakresu merytorycznego prac. Akceptacja planu audytu fizycznego na obiekcie.
 - Zmapowanie zapisów dokumentacji ze środowiskiem fizycznym
 - Przegląd procesów głównych i wspomagających, zadań jednostki, czynności stanowiskowych, rodzajów informacji (pod kątem cyberbezpieczeństwa), u Zamawiającego.
 - Przegląd infrastruktury IT w stopniu wymaganym do przeprowadzenia analiz.
 - Wywiady z pracownikami zakładu
 - Konsultacje z kadrą zarządzającą obszarami merytorycznymi
 - Miejsce realizacji prac fazy
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY
- Inwentaryzacja musi być wykonana pod kątem późniejszego projektowania koncepcyjnego
- Zakres ogólny
 - Obszary podlegające opracowaniu:
 - Systemy skomputeryzowane
 - Komunikacja sieciowa
 - Monitoring systemów i transmisji danych
 - Interfejsy systemowe
 - Miejsce realizacji prac
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO oraz
 - Biuro WYKONAWCY

2.3. DOKUMENTACJA - PRODUKTY POSZCZEGÓLNYCH ETAPÓW

- Produkt
 - Dokumentacja inwentaryzacyjna i analityczna.
- Format
 - Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku do wyboru docx, odt, vpp).
- Sposób dostarczenia produktu
 - Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
 - Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego
- Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO lub
- Biuro WYKONAWCY
- Inwentaryzacja obiektów fizycznych w formie Audytu
 - Obszary podlegające opracowaniu
 - Systemy skomputeryzowane
 - Komunikacja
 - Interfejsy systemowe
 - Opis projektowanych systemów IT
 - Wytyczne i wymagania producentów poszczególnym komponentów głównych
 - Format
 - Pisemny, w edytowalnej formie elektronicznej (format pliku docx, odt, vpp).
 - Mapa połączeń wykonana zgodnie z notacją Archimate 2.0 lub nowszą
 - Sposób dostarczenia produktu
 - Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
 - Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego ZAMAWIAJĄCEGO produktów projektu
 - Miejsce realizacji prac
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY

2.4. Zakres szczegółowy inwentaryzacji

- Inwentaryzacja ma być wykonana do poziomu urządzeń aktywnych systemów AKPiA
- Dokumentacja inwentaryzacyjna ma zawierać:
 - Topologię logiczną sieci warstwy 2
 - Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
 - Eksport do wektorowego PDF
 - Topologia ma zawierać urządzenia ze źródłowymi adresami MAC i wskazaniem portu fizycznego urządzeń sąsiedzkich (np. komputer <-> przełącznik)
 - Topologia ma być ograniczona do punk tu styku z operatorami zewnętrznymi
 - Topologię logiczną sieci warstwy 3
 - Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
 - Eksport do wektorowego PDF
 - Topologia ma zawierać urządzenia ze źródłowymi adresami MAC i wskazaniem portu fizycznego urządzeń sąsiedzkich (np. komputer <-> przełącznik)
 - Topologia ma być ograniczona do punk tu styku z operatorami zewnętrznymi
 - Mapę komunikacji – oznaczenie obiektów, które wymieniają między sobą dane
 - Forma tabelaryczna z oznaczeniem MAC oraz IPv4 źródła i przeznaczenia. W przypadku routingu oznaczyć MAC interfejsu wyjściowego routera jako adres przypisany do IP źródłowego. Wykazać w tabeli powiązanie IP do wielu adresów

- MAC (jeden sprzętowy źródła oraz wszystkie adresy MAC interfejsów wyjściowych routerów w całej ścieżce komunikacyjnej do miejsca docelowego).
- Ustawienia reguł Firewalli
 - Forma tabelaryczna w formacie xlsx lub zgodnym
 - Ujęcie urządzenia, wirtualizacji jeśli istnieje, zapisu reguły, status (aktywna lub nie aktywna) efekt działania,
- Listy komponentów
 - Forma tabelaryczna w formacie xlsx lub zgodnym
- Zestawienie musi zawierać minimum, model, lokalizacja, miejsce montażu, numer seryjny lub numer inwentarzowy (jeżeli urządzenie wymaga demontażu – nie dokonujemy tej czynności a numery seryjne lub model pozostawiamy niewypełniony) adres MAC, adres IP, przypisanie do systemu dziedzicznego, właściciel systemu (osoba lub osoby odpowiedzialne za działanie komponentu)
- Ustawienia zasad dostępu do zasobów do poziomu stacji roboczych i użytkowników
 - Forma tabelaryczna w formacie xlsx lub zgodnym
 - Wylistowanie użytkowników oraz zasobów sieciowych wraz z przypisaniem do komponentu (jeśli dotyczy) oraz systemu docelowego do poziomu adresu IPv4

Zadanie 31. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT – montaż RACK 19” (dedykowane urządzenia do analizy protokołów przemysłowych)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuk urządzenia przeznaczonego do ochrony i monitorowania środowisk OT, w postaci platform sprzętowej – urządzenia aktywnego sieci, przystosowanych do montażu w standardzie RACK, wraz z funkcjonalnościami z zakresu bezpieczeństwa teleinformatycznego, zgodnie z wymaganiami technicznymi i funkcjonalnymi określonymi przez Zamawiającego.

2. Wymagania dotyczące rozwiązania

2.1. Wymagania ogólne dla sprzętu:

- musi być nowy (nie starszy niż z 4 kwartału 2025 r) i pochodzić z polskiego kanału dystrybucji
- musi posiadać gwarancję i wsparcie producenta na okres nie krótszy niż do 30.06.2026
- producent musi zapewnić czas życia produktu do końca roku 2032 roku. Nie dopuszcza się rozwiązań będących w okresie zakończenia życia (end-of-life) lub zakończenia wsparcia (end-of-support) lub zakończenia sprzedaży (end-of-sale).

2.2. Wymagania ogólne dla urządzeń aktywnych sieci

- Urządzenia montowane do szaf rack 19” muszą:
 - Posiadać dwa zasilacze 230 V działające w układzie nadmiarowym i uzupełniającym

- o Posiadać strukturę modułową (nie dopuszcza się sprzętu które nie posiada chociaż jednego modułu rozszerzeń do którego można dołożyć – po za projektem np. dodatkowy moduł komunikacyjny np. interfejsy Ethernet 8x 1 Gb/S SFP)
- o Posiadać aktualny certyfikat IEC 62443 4-2 SL4 akredytowany przez PCA
- o Urządzenia muszą stanowić platformę bezpieczeństwa obok standardowych funkcjonalności urządzeń aktywnych sieci takich jak przełączanie czy routing L3.
- o Być montowane na szynach wysuwanych umożliwiając łatwy dostęp do górnej części urządzenia
- o Muszą posiadać certyfikat FCC Class A, CE, UL
- o Komplet wymieniony poniżej w ilości: 1 szt

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 32 GB	1
Storage	Min. 900 GB	2
Interfejs MGMT	RJ45	1
Interfejs Szeregowy	Konsola RS232 – RJ45	1
Zasilacze	230 V	2
Interfejs 10 Gb/s	SFP+ Ethernet	4
Wkładki	SFP+ 10 Gb/s SM	2
Interfejs 1 Gb/s	RJ45 Ethernet with bypass	16
Interfejs 1 Gb/s	RJ45 Ethernet with out bypass	8
Interfejs 1 Gb/s	SFP 1 Gb/s	8
Wkładki 1 Gb/s	SFP 1 Gb/s SM	8

Szyny montażowe	Rail, teleskopowe, do szaf 19"	1
Kable zasilające	Min 1,5 m	2
Typ montażu	Do szafy 19", wysokość max 2 U	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	16
Patch cordy	Światłowodowe SC/LC 1,5 m SM	4
Montaż	Do szafy Rack 19", szyny rail, teleskopowe	n/d
Konsola centralna	Zarządzanie Firewall z poziomu konsoli centralnej zintegrowanej z centralnym systemem SIEM/IDS, pochodząca od tego samego producenta co urządzenie aktywne	n/d

2.3. Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

- Routing i przełączanie (L2 / L3)
 - Pełny routing IPv4 i IPv6 (statyczny, dynamiczny, policy-based, VRF).
 - Obsługa protokołów routingu: OSPFv2/v3, BGP, RIP, RIPng, Babel, IS-IS.
 - VRRP – redundancja bramy sieciowej (High Availability).
 - MPLS / VPLS / LDP / RSVP – wsparcie dla sieci operatorskich i segmentacji.
 - Policy-Based Routing (PBR) – wybór trasy na podstawie źródła, portu, typu ruchu.
 - Ethernet bridging (L2) – możliwość pracy jako przełącznik (bridge, VLAN, trunk).
 - STP / RSTP – obsługa protokołów zapobiegających pętlom w sieci.
 - 802.1Q VLAN / QinQ – pełne wsparcie dla VLAN i tunelowania VLAN w VLAN.
 - LACP / Bonding / Port-channel – łączenie interfejsów dla redundancji i wydajności.
 - VRF / Route Tables – separacja ruchu i izolacja sieci logicznych.
- Firewall i bezpieczeństwo

- Stateful Firewall (ZBFW – Zone-Based Firewall) – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
- NAT (Source, Destination, Static, Masquerade) – pełna translacja adresów.
- Policy NAT i Hairpin NAT – elastyczne mapowanie adresów w zależności od kierunku.
- IPv6 Firewall – osobne polityki bezpieczeństwa dla IPv6.
- Traffic Filtering na poziomie L2–L4 – filtrowanie pakietów, portów, protokołów.
- Time-based Rules – polityki bezpieczeństwa zależne od czasu.
- Conntrack / Helper modules – śledzenie sesji i stanów połączeń.
- Rate-limiting / DoS protection – ograniczanie przepustowości, ochrona przed floodem.
- MAC Firewall / ARP Inspection / Static ARP tables – kontrola komunikacji warstwy drugiej.
- VPN i tunelowanie
 - IPsec IKEv1 / IKEv2 – szyfrowane tunele site-to-site i remote access.
 - L2TP, PPTP, OpenVPN, WireGuard – elastyczne protokoły VPN dla użytkowników i urządzeń.
 - GRE / mGRE / VTI / VXLAN / IP-in-IP – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
 - Dynamiczny routing przez VPN (BGP over IPsec) – skalowalność w dużych sieciach.
 - DMVPN V3 – automatyka zestawiania topologii HUB Spoke z zabezpieczaniem IPsec i protokołami routingu wraz z protokołem NHRP
 - SSL VPN / Remote Access – wsparcie dla zdalnego dostępu użytkowników.
- QoS i kontrola ruchu
 - Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC) – kontrola pasma.
 - Hierarchical QoS (HQoS) – wielopoziomowe kolejkovanie.
 - Traffic Classification (DSCP / CoS / ACL match) – klasyfikacja ruchu na podstawie atrybutów.
 - Bandwidth Management per interface / per VLAN – kontrola przepustowości per-port lub per-sieć.
- Monitoring, logowanie i diagnostyka
 - SNMP v1/v2c/v3 – monitorowanie zewnętrzne.
 - Syslog (lokalny i zdalny) – pełna integracja logów z systemami SIEM/IDS.
 - NetFlow / sFlow / IPFIX – eksport statystyk ruchu do systemów analitycznych.
 - Ping / Traceroute / MTR / Packet Capture (tcpdump) – diagnostyka sieciowa.
 - BFD – szybkie wykrywanie awarii tras routingu.
 - Interface Counters / Flow statistics – bieżące statystyki ruchu.
 - Monitorowanie w trybie inline – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
 - Mirror Port – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
 - Przekierowanie wewnętrzne do systemów analityki – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyka ochrony inline

- Analityka anomalii komunikacji sieciowej pomiędzy komponentami
- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT
- Wbudowany system traceability dla monitorowania głębokich danych do poziomu nastaw i wartości np. rejestrów
- Zarządzanie i automatyzacja
 - CLI / SSH / API / RESTCONF / NETCONF – wielowarstwowe zarządzanie.
 - Konfiguracja CLI w stylu Cisco / Juniper – logiczne drzewo konfiguracji.
 - Atomic commits / rollback / diff – bezpieczne zmiany i cofanie konfiguracji.
 - Scheduled tasks / cron / event-driven scripts – automatyzacja procesów.
 - Ansible / Salt / Terraform ready – zgodność z narzędziami DevOps.
 - Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP – kontrola dostępu administracyjnego.
 - Backup / restore / config versioning – bezpieczeństwo konfiguracji.
 - Zarządzanie Firewall – wymagane jest również zarządzanie z poziomu konsoli centralnej

2.4. IDS/IPS

- Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.
 - Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)
 - Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
 - Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
 - Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.

- Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
- Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
- Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagłe wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów, SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji
 - Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - Aktywacja polityk obronnych w firewallu
 - Dynamiczne uczenie się ruchu sieciowego (profilowanie).
 - Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM/IDS.
 - Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.

- Możliwość integracji z pulpitami centralnego SIEM/IDS .
- Dodatkowe moduły
 - DHCP server/relay/client, DNS server/forwarder, NTP, HTTP proxy, NetBIOS relay.
 - Dynamic DNS, Static Hosts, Name-resolution cache.
 - Multicast routing (PIM/IGMP).
 - IPv6 autoconfiguration / router advertisement (RA).
 - System High Availability (VRRP, Sync) – redundancja i przełączenie awaryjne.
 - Zarządzanie certyfikatami SSL / PKI – obsługa CA, kluczy i certyfikatów.
- Dodatkowe cechy
 - Rolling Release – aktualizacje bezpieczeństwa w cyklu ciągłym.
 - Integracja z Docker / LXC / KVM – uruchamianie usług w kontenerach.

Obsługa Netfilter nftables / eBPF – nowoczesne mechanizmy filtrowania.

GWARANCJA – 24 miesiące

Zadanie 32. Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuk dedykowanych urządzeń sprzętowych w postaci sond/sensorów do monitorowania sieci OT (Operational Technology), umożliwiających analizę komunikacji oraz identyfikację zdarzeń w zakresie protokołów przemysłowych, zgodnych z wymaganiami technicznymi określonymi w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania

2.1. Wymagania ogólne dla sprzętu:

- musi być nowy (nie starszy niż z 4 kwartału 2025 r) i pochodzić z polskiego kanału dystrybucji
- musi posiadać gwarancję i wsparcie producenta na okres nie krótszy niż do 30.06.2026
- producent musi zapewnić czas życia produktu do końca roku 2032 roku. Nie dopuszcza się rozwiązań będących w okresie zakończenia życia (end-of-life) lub zakończenia wsparcia (end-of-support) lub zakończenia sprzedaży (end-of-sale).

2.2. Wymagania ogólne dla urządzeń aktywnych sieci

Urządzenia montowane na szynę DIN35mm muszą:

- Być dostarczone z dwoma zasilaczami 230 V / DC 24 V dostosowane mocowo do dostarczanych urządzeń działające w układzie nadmiarowym i uzupełniającym
- Posiadać aktualny certyfikat IEC 62443 4-2 SL4 akredytowany przez PCA
- Urządzenia muszą stanowić platformę bezpieczeństwa obok standardowych funkcjonalności urządzeń aktywnych sieci takich jak przełączanie czy routing L3.
- Być montowane na szynach wysuwanych umożliwiając łatwy dostęp do górnej części urządzenia
- Muszą posiadać certyfikat FCC Class A, CE, UL
- W przypadku montażu w podstawach elektroenergetycznych wymagane są dodatkowo certyfikaty na sprzęt IEEE 1613, C1D2, IEC 61850-3, CB

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 8 GB	1
Storage	Min. 480 GB	1
Interfejs Szeregowy	Konsola RS232	1
Zasilacze	230 V 5 A – 24 V DC	2
Interfejs 1 Gb/s	Min RJ45 Ethernet 2 porty bypass Min RJ45 Ethernet 2 porty pracujące bez bypass	Minimum 2 pracujące w trybie bypass (utrzymanie łączności w przypadku braku zasilania)
Interfejs 1 Gb/s	SFP 1 Gb/s	Minimum 2 x SFP 1 Gb/s.
Wkładki 1 Gb/s	SFP 1 Gb/s	2 sztuki – parametry: 10 KM 1310 nm SM
Uchwyty montażowe	1 komplet dla DIN35	1
Kable zasilające	Min 0,5 m	2

Typ montażu	Szyna DIN35	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	2
Patch cordy	Światłowodowe SC/LC 1,5 m SM PC/APC LC-LC	2
Konsola centralna	Zarządzanie Firewall z poziomu konsoli centralnej zintegrowanej z centralnym systemem SIEM/IDS, pochodząca od tego samego producenta co urządzenie aktywne	n/d
Certyfikaty wymagane	CE, FCC Class A, UL, IEC 62443 4-2 SL4, IEC 62443 4-2 SL4	n/d
Temperatura pracy	Od minus 40 stopni Celsjusza do plus 70 stopni Celsjusza	

2.3. Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

- Routing i przełączanie (L2 / L3)
 - Pełny routing IPv4 i IPv6 (statyczny, dynamiczny, policy-based, VRF).
 - Obsługa protokołów routingu: OSPFv2/v3, BGP, RIP, RIPng, Babel, IS-IS.
 - VRRP – redundancja bramy sieciowej (High Availability).
 - MPLS / VPLS / LDP / RSVP – wsparcie dla sieci operatorskich i segmentacji.
 - Policy-Based Routing (PBR) – wybór trasy na podstawie źródła, portu, typu ruchu.
 - Ethernet bridging (L2) – możliwość pracy jako przełącznik (bridge, VLAN, trunk).
 - STP / RSTP – obsługa protokołów zapobiegających pętlom w sieci.
 - 802.1Q VLAN / QinQ – pełne wsparcie dla VLAN i tunelowania VLAN w VLAN.
 - LACP / Bonding / Port-channel – łączenie interfejsów dla redundancji i wydajności.
 - VRF / Route Tables – separacja ruchu i izolacja sieci logicznych.
- Firewall i bezpieczeństwo
 - Stateful Firewall (ZBFW – Zone-Based Firewall) – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
 - NAT (Source, Destination, Static, Masquerade) – pełna translacja adresów.

- Policy NAT i Hairpin NAT – elastyczne mapowanie adresów w zależności od kierunku.
- IPv6 Firewall – osobne polityki bezpieczeństwa dla IPv6.
- Traffic Filtering na poziomie L2–L4 – filtrowanie pakietów, portów, protokołów.
- Time-based Rules – polityki bezpieczeństwa zależne od czasu.
- Conntrack / Helper modules – śledzenie sesji i stanów połączeń.
- Rate-limiting / DoS protection – ograniczanie przepustowości, ochrona przed floodem.
- MAC Firewall / ARP Inspection / Static ARP tables – kontrola komunikacji warstwy drugiej.
- VPN i tunelowanie
 - IPsec IKEv1 / IKEv2 – szyfrowane tunele site-to-site i remote access.
 - L2TP, PPTP, OpenVPN, WireGuard – elastyczne protokoły VPN dla użytkowników i urządzeń.
 - GRE / mGRE / VTI / VXLAN / IP-in-IP – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
 - Dynamiczny routing przez VPN (BGP over IPsec) – skalowalność w dużych sieciach.
 - DMVPN V3 – automatyka zestawiania topologii HUB Spoke z zabezpieczeniem IPsec i protokołami routingu wraz z protokołem NHRP
 - SSL VPN / Remote Access – wsparcie dla zdalnego dostępu użytkowników.
- QoS i kontrola ruchu
 - Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC) – kontrola pasma.
 - Hierarchical QoS (HQoS) – wielopoziomowe kolejkovanie.
 - Traffic Classification (DSCP / CoS / ACL match) – klasyfikacja ruchu na podstawie atrybutów.
 - Bandwidth Management per interface / per VLAN – kontrola przepustowości per-port lub per-sieć.
- Monitoring, logowanie i diagnostyka
 - SNMP v1/v2c/v3 – monitorowanie zewnętrzne.
 - Syslog (lokalny i zdalny) – pełna integracja logów z systemami SIEM/IDS.
 - NetFlow / sFlow / IPFIX – eksport statystyk ruchu do systemów analitycznych.
 - Ping / Traceroute / MTR / Packet Capture (tcpdump) – diagnostyka sieciowa.
 - BFD – szybkie wykrywanie awarii tras routingu.
 - Interface Counters / Flow statistics – bieżące statystyki ruchu.
 - Monitorowanie w trybie inline – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
 - Mirror Port – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
 - Przekierowanie wewnętrzne do systemów analityki – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyką ochrony inline
 - Analityka anomalii komunikacji sieciowej pomiędzy komponentami

- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT
- Wbudowany system traceability dla monitorowania głębokich danych do poziomu nastaw i wartości np. rejestrów
- Zarządzanie i automatyzacja
 - CLI / SSH / API / RESTCONF / NETCONF – wielowarstwowe zarządzanie.
 - Konfiguracja CLI w stylu Cisco / Juniper – logiczne drzewo konfiguracji.
 - Atomic commits / rollback / diff – bezpieczne zmiany i cofanie konfiguracji.
 - Scheduled tasks / cron / event-driven scripts – automatyzacja procesów.
 - Ansible / Salt / Terraform ready – zgodność z narzędziami DevOps.
 - Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP – kontrola dostępu administracyjnego.
 - Backup / restore / config versioning – bezpieczeństwo konfiguracji.
 - Zarządzanie Firewall – wymagane jest również zarządzanie z poziomu konsoli centralnej

2.4. IDS/IPS - Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.

- Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)
 - Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).
 - Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
 - Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.

- Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
- Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
- Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagle wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.
- Mechanizmy automatyzacji i korelacji
 - Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - Aktywacja polityk obronnych w firewallu .
 - Dynamiczne uczenie się ruchu sieciowego (profilowanie).
 - Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM/IDS.
 - Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
 - Możliwość integracji z pulpitemi centralnego SIEM/IDS .

2.5. Dodatkowe moduły

- DHCP server/relay/client, DNS server/forwarder, NTP, HTTP proxy, NetBIOS relay.
- Dynamic DNS, Static Hosts, Name-resolution cache.
- Multicast routing (PIM/IGMP).
- IPv6 autoconfiguration / router advertisement (RA).

- System High Availability (VRRP, Sync) – redundancja i przełączenie awaryjne.
- Zarządzanie certyfikatami SSL / PKI – obsługa CA, kluczy i certyfikatów.

2.6. Dodatkowe cechy

- Rolling Release – aktualizacje bezpieczeństwa w cyklu ciągłym.
- Integracja z Docker / LXC / KVM – uruchamianie usług w kontenerach.

Obsługa Netfilter nftables / eBPF – nowoczesne mechanizmy filtrowania.

Gwarancja 24 miesiące

Zadanie 33. Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT. Oprogramowanie platformowe, zintegrowany System bezpieczeństwa IPS/IDS, OT Anomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat), SIEM, AKPiA RSDT, XDR, NDR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 sztuki oprogramowania dedykowanego do detekcji zagrożeń i monitorowania bezpieczeństwa sieci OT, wraz z kompletem licencji niezbędnych do jego pełnego uruchomienia, konfiguracji oraz eksploatacji, zgodnie z wymaganiami technicznymi i funkcjonalnymi określonymi przez Zamawiającego.

1. Wymagania dotyczące rozwiązania

2.1. Centralny system bezpieczeństwa

- Preferuje się system zintegrowany z jedną konsolą zarządzającą dla poniższych grup funkcyjnych.
- Dopuszcza się stosowanie wielu rozwiązań, pod warunkiem integracji umożliwiającej wizualizację danych na centralnych pulpitach bezpieczeństwa, bez konieczności uruchamiania dedykowanych konsol dla pozostałych systemów wchodzących w skład architektury.
- Wymaga się aby wszystkie zastosowane grupy programowe nie miały ograniczeń licencyjnych na ilość przetwarzanych danych, ilość adresów IP czy MAC.

2.2. System SIEM/IDS

Parametr	Opis / wartość parametru	Ilość
Ilość użytkowników	Ilość jednoczesnych logowań Ilość licencjonowanych użytkowników	Bez ograniczeń licencyjnych
Okres objęty licencją	Licencja bezterminowa czasowo	n/d
Dostęp dla użytkownika	Przez przeglądarkę internetową	n/d
Projektowanie widoczności danych	Poprzez interfejs GUI	n/d
Pulpity operacyjne	Ilość możliwych pulpitów do wprowadzenia	Bez ograniczeń
Ilość instancji	Ilość wymaganych instalacji przez Zamawiającego	1
Miejsce instalacji	Lokalna u Zamawiającego	n/d
Instalacja chmurowa	Nie dopuszczalna	n/d

Wymagana integracja	ITSM, XDR	n/d
Wsparcie AI	TAK	U dostawcy lub lokalnie

2.3. Opis ogólny

- Wymagany system powinien stanowić centralny panel wizualizacji stanu bezpieczeństwa OT i aktywności systemu cyberbezpieczeństwa. Musi umożliwiać operatorowi SOC (Security Operations Center) lub administratorowi IT/OT szybki wgląd w sytuację bezpieczeństwa, liczbę zdarzeń, alarmów oraz aktywność urządzeń w sieci.
- Zamawiający oczekuje zintegrowanego systemu klasy SIEM/CMDB/IDS/Asset/NSPM dla środowisk przemysłowych, łączącym funkcje bezpieczeństwa, inwentaryzacji i zarządzania politykami w jednym środowisku. System musi być zaprojektowany specjalnie dla infrastruktury OT/ICS i oferować pasywne monitorowanie, automatyczną analizę, raportowanie ryzyka i korelację zdarzeń bez domyślnej ingerencji w proces produkcyjny.

2.4. Wymagane minimalne funkcjonalności systemu SIEM/IDS:

- Monitoring i korelacja zdarzeń (SIEM / IDS)
 - Centralna baza wszystkich zdarzeń z systemów IT, OT i IoT.
 - Korelacja logów z różnych źródeł (firewalle, routery, IDS, serwery, PLC).
 - Wykrywanie i grupowanie incydentów bezpieczeństwa.
 - Analiza w czasie rzeczywistym z klasyfikacją ryzyka (niski/średni/wysoki).
 - Automatyczna identyfikacja powiązanych zasobów i relacji między nimi.
 - Widok szczegółów alarmu: reguła, czas, źródło, typ, ryzyko, status.
 - Integracja z silnikiem reguł alarmowych (Zasady alarmowe).
 - Wsparcie dla korelacji według MITRE ATT&CK (np. T1040, T1071).
 - Pełna historia i oś czasu zdarzeń (timeline).
 - Możliwość filtrowania, eksportu i analizy porównawczej.
- System alarmowy (IDS/IPS/Anomalie sieciowe)
 - Wykrywanie anomalii sieciowych w oparciu o sygnatury i heurystykę.
 - Detekcja nieautoryzowanego ruchu, nietypowych portów i protokołów.
 - Identyfikacja potencjalnych prób eksfiltracji danych lub sniffingu.
 - Integracja z modulem Network Anomalies.
 - Wsparcie dla CVE i korelacja podatności (np. CVE-2020-0796).
 - Klasyfikacja alarmów wg typu i priorytetu ryzyka.
 - Mapowanie powiązanych zasobów i adresów IP/MAC.
 - Powiązanie alarmów z konkretnymi urządzeniami
 - Możliwość ręcznego lub automatycznego zamykania alarmów.

- Historia alarmów i statusów (aktywny, ponownie otwarty, zamknięty).
- Inwentarz zasobów (Asset & CMDB)
 - Automatyczna identyfikacja zasobów w sieci (adres MAC, IP, model, OS).
 - Profilowanie urządzeń i przypisywanie ich do grup lub sieci.
 - Baza konfiguracji sprzętowych i programowych (CPU, RAM, porty, OS).
 - Klasyfikacja urządzeń: ICS Dev, Router, Switch, Serwer, Host, SCADA itp.
 - Przypisywanie wartości aktywa (1–10) oraz poziomu ryzyka.
 - Rejestr zdarzeń powiązanych z zasobem.
 - Historia zmian konfiguracji i aktualizacji.
 - Wbudowany edytor zasobu i przypisanie do sieci/peryferii.
 - Możliwość dodania notatek technicznych lub operacyjnych.
 - Integracja z modulem *Diagram PERA* — wizualizacja topologii.
- Profile komunikacyjne (Network Behavior Profiling)
 - Tworzenie profili zachowań sieciowych dla każdego adresu MAC.
 - Rejestr interfejsów, ruchu i komunikacji między urządzeniami.
 - Analiza różnic w zachowaniu (detekcja odchyleń od normy).
 - Automatyczne tworzenie i aktualizacja profili.
 - Eksport listy profili do raportów i porównań audytowych.
 - Wizualne odwzorowanie relacji z urządzeniami aktywnymi sieci tego samego producenta co system SIEM/IDS
- Analiza danych i ryzyka
 - Automatyczna analiza zidentyfikowanych anomalii.
 - Raporty o potencjalnych wektorach ataku (MITRE ATT&CK).
 - Wskazanie nieautoryzowanych portów i usług.
 - Analiza zgodności z IEC 62443 i ISO 27001.
 - Raport z zaleceniami: „Zagrożenia – Konsekwencje – Działania”.
 - Ocena ryzyka braku działań korygujących (np. w 90 dni).
 - Szacowanie wpływu incydentu na zasoby i infrastrukturę.
- Wizualizacja i topologia sieci (Diagram PERA)
 - Automatyczna mapa relacji między zasobami i segmentami sieci.
 - Kolorystyczne oznaczenia poziomu ryzyka i statusu połączeń.
 - Możliwość interakcji z elementami (kliknięcie → szczegóły zasobu).
 - Integracja z danymi z modułów *Zdarzenia* i *Alarmy*.
 - Widok struktury per strefy PERA (Enterprise / Control / Field / DMZ).
- Zasady alarmowe i polityki bezpieczeństwa (NSPM)
 - Definiowanie reguł alarmowych (np. porty, IP, usługi, typ zdarzenia).
 - Priorytetyzacja zasad i poziomu alarmowe.
 - Automatyczne uruchamianie alarmów po spełnieniu warunków.
 - Możliwość wyciszania określonych alarmów lub źródeł.
 - Integracja z tabelą interfejsów i reguł firewall dostarczonych urządzeń bezpieczeństwa OT
 - Pełna zgodność z architekturą Zone-Based Firewall.

- Raportowanie i analityka
 - Generowanie raportów z analizy ryzyka i podatności.
 - Podsumowania incydentów i trendów zagrożeń.
 - Raporty dla audytów (IEC 62443, ISO 27001, ISO 22301).
 - Możliwość eksportu do PDF, CSV.
 - Raporty z przypisaniem do zasobów, sieci i alarmów.
- Integracja z urządzeniami aktywnymi sieci
 - System musi zapewniać natywną integrację z urządzeniami bezpieczeństwa tego samego producenta umożliwiającą synchronizację polityk bezpieczeństwa oraz jednocześnie umożliwiać integrację z urządzeniami innych producentów poprzez standardowe mechanizmy wymiany danych.
 - Odczyt metadanych sprzętowych (model, CPU, pamięć, porty, firmware).
 - Monitorowanie stanu portów, interfejsów i komunikacji L2/L3.
 - Wykorzystanie urządzeń aktywnych sieci tego samego producenta jako źródeł danych IDS i monitoringu sieciowego.
 - Wykorzystanie urządzeń aktywnych sieci dowolnego producenta który umożliwia wysyłanie zdarzeń, kopii ruchu (poprzez sondy danych tego samego producenta), logowań, danych z sflow/netflow jako źródeł danych dla SIEM/IDS
 - Synchronizacja polityk bezpieczeństwa między systemem a urządzeniami aktywnymi tego samego producenta
- Dodatkowe funkcje operacyjne
 - Historia działań administratora (logi operacyjne).
 - Panel użytkownika i uprawnienia administracyjne.
 - Przegląd wszystkich interfejsów sieciowych i tabeli firewall.
 - Możliwość wizualizacji alarmów w czasie rzeczywistym (Alarms live).
 - Panel wydajności systemu (monitor CPU, pamięci, dysków).
 - Integracja z modułem raportów dziennych / tygodniowych.
 - Mechanizmy wykluczeń i filtrów do analizy danych.
- Normy, zgodność i audyt
 - Zgodność z normami IEC 62443, ISO 27001, ISO 22301.
 - Struktura raportów i klasyfikacja ryzyk zgodna z IEC 62443-3-3.
 - Analiza niezgodności i rekomendacje działań korygujących.
 - Mapowanie do wymagań bezpieczeństwa OT i IT.
- Architektura i integracja
 - Działanie w środowisku Linux / Vmware / HyperV / KVM / Proxmox lub na dedykowanym Appliance sprzętowym – certyfikowanym IEC 62443 4-2 SL4
 - Baza danych typu SQL
 - Możliwość pracy w środowiskach mieszanych (OT, IT)
 - API do integracji z zewnętrznymi systemami.
 - Zdalna administracja i aktualizacje systemu.
- Wyróżniki unikalne
 - Dedykowane dla środowisk OT / ICS / SCADA.

- Brak komponentów wymagających dodatkowych licencji.
- Pełna integracja z fizycznymi urządzeniami aktywnymi sieci tego samego producenta.
- Wysoka czytelność interfejsu – jeden panel łączący SIEM, Asset i NSPM.
- Polski interfejs
- Polskie komunikaty w szczególności dane analityczne
- Analiza anomalii ruchu sieciowego
 - System musi umożliwiać wykrywanie anomalii w ruchu sieciowym na podstawie:
 - analizy statystycznej
 - profili komunikacyjnych urządzeń
 - relacji komunikacyjnych pomiędzy zasobami
 - System musi umożliwiać identyfikację:
 - nietypowych źródeł ruchu
 - nietypowych usług
 - nietypowych portów komunikacyjnych
 - anomalii wolumetrycznych
 - System musi prezentować wyniki w postaci:
 - rankingów
 - statystyk
 - wizualizacji rozkładu ruchu
- Dynamiczne mapy zależności komunikacyjnych. System musi umożliwiać generowanie dynamicznych map komunikacji pomiędzy zasobami w sieci.
 - Mapa musi umożliwiać:
 - wizualizację relacji pomiędzy adresami IP
 - wizualizację relacji pomiędzy adresami MAC
 - identyfikację centralnych węzłów komunikacyjnych
 - analizę kierunków przepływu danych
 - System musi umożliwiać analizę grafową obejmującą:
 - powiązania pomiędzy zasobami
 - intensywność komunikacji
 - topologię relacji
- Automatyczne modelowanie topologii sieci
 - System musi automatycznie tworzyć i aktualizować:
 - diagramy fizycznej topologii sieci
 - relacje pomiędzy urządzeniami
 - powiązania interfejsów sieciowych
 - System musi umożliwiać:
 - wizualizację urządzeń sieciowych
 - identyfikację interfejsów
 - identyfikację połączeń fizycznych
 - identyfikację połączeń logicznych
 - Diagram musi być:

- dynamiczny
 - aktualizowany automatycznie
 - powiązany z rzeczywistymi zdarzeniami sieciowymi.
-
- Inwentaryzacja zasobów OT i IT
 - System musi zapewniać automatyczną inwentaryzację zasobów obejmującą:
 - adres IP
 - adres MAC
 - nazwę hosta
 - producenta urządzenia
 - model urządzenia
 - typ urządzenia
 - rolę w sieci
 - System musi umożliwiać klasyfikację zasobów co najmniej jako:
 - urządzenia OT
 - urządzenia IT
 - urządzenia sieciowe
 - stacje robocze
 - serwery
 - urządzenia przemysłowe.
 - Profile komunikacyjne zasobów
 - System musi umożliwiać tworzenie profili komunikacyjnych urządzeń.
 - Profil musi obejmować co najmniej:
 - typowe kierunki komunikacji
 - wykorzystywane porty
 - wykorzystywane protokoły
 - wolumen komunikacji
 - System musi umożliwiać wykrywanie odchyleń od profilu.
 - Analiza zdarzeń powiązanych z zasobami
 - System musi umożliwiać analizę zdarzeń w kontekście konkretnego zasobu obejmującą:
 - historię zdarzeń
 - powiązane zasoby
 - zdarzenia sieciowe
 - zdarzenia bezpieczeństwa
 - Analiza musi być dostępna z poziomu:
 - widoku zasobu

- widoku zdarzeń
 - widoku analitycznego.
- Korelacja zdarzeń bezpieczeństwa
 - System musi zapewniać możliwość budowania mechanizmów korelacji zdarzeń w oparciu o:
 - sekwencje zdarzeń
 - liczbę wystąpień zdarzeń
 - zależności pomiędzy zdarzeniami
 - zależności czasowe.
 - Mechanizm korelacji musi umożliwiać:
 - budowę scenariuszy detekcji
 - budowę playbooków
 - definiowanie progów zdarzeń.
- Graficzny edytor playbooków bezpieczeństwa
 - System musi umożliwiać tworzenie procedur detekcji i reakcji w postaci graficznych diagramów logicznych.
 - Edytor musi umożliwiać:
 - definiowanie filtrów zdarzeń
 - tworzenie liczników zdarzeń
 - definiowanie progów alarmowych
 - budowę scenariuszy korelacji
- Alarmowanie i zarządzanie incydentami
 - System musi umożliwiać generowanie alarmów bezpieczeństwa na podstawie:
 - reguł korelacyjnych
 - wykrytych anomalii
 - zdarzeń bezpieczeństwa
 - Alarm musi zawierać:
 - poziom wiarygodności
 - liczbę zdarzeń powiązanych
 - listę zasobów powiązanych
- Analiza wolumenów zdarzeń
 - System musi umożliwiać analizę wolumenów zdarzeń obejmującą:
 - zdarzenia na sekundę
 - zdarzenia na urządzenie
 - zdarzenia na typ zdarzenia
 - System musi umożliwiać wizualizację trendów zdarzeń w czasie.
- Wizualizacja przepływów zdarzeń
 - System musi umożliwiać wizualizację przepływu zdarzeń pomiędzy:
 - źródłami danych
 - modułami analitycznymi
 - mechanizmami korelacyjnymi
 - systemem alarmowym.

- Model hierarchiczny infrastruktury (rozszerzony model PERA)
 - System musi umożliwiać modelowanie infrastruktury w oparciu o hierarchiczny model architektury przemysłowej, obejmujący co najmniej:
 - poziomy modelu Purdue (PERA)
 - strefy logiczne systemów OT/IT
 - lokalizacje fizyczne
 - jednostki organizacyjne.
 - System musi umożliwiać zagnieżdżanie kontenerów infrastruktury, pozwalające na grupowanie zasobów według:
 - lokalizacji geograficznych
 - budynków
 - pomieszczeń
 - stref technologicznych
 - poziomów architektury przemysłowej.
 - Kontenery muszą umożliwiać tworzenie hierarchicznych struktur wielopoziomowych
- Telemetria infrastruktury
 - System musi umożliwiać zbieranie oraz wizualizację parametrów telemetrycznych infrastruktury obejmujących co najmniej:
 - obciążenie CPU
 - wykorzystanie pamięci RAM
 - wykorzystanie przestrzeni dyskowej
 - średnie obciążenie systemu.
 - System musi umożliwiać analizę telemetryczną w czasie rzeczywistym oraz historyczną.
 - System musi umożliwiać wizualizację parametrów w postaci:
 - wykresów czasowych
 - rankingów zasobów
 - map obciążenia infrastruktury.
- Centralne zarządzanie polityką bezpieczeństwa sieci
 - System musi umożliwiać centralne zarządzanie polityką bezpieczeństwa sieci obejmującą urządzenia filtrujące ruch sieciowy.
 - System musi umożliwiać:
 - przegląd reguł bezpieczeństwa
 - analizę relacji pomiędzy regułami
 - analizę wykorzystania reguł
 - identyfikację reguł nieużywanych.
 - System musi umożliwiać analizę reguł bezpieczeństwa w kontekście:
 - źródła komunikacji
 - celu komunikacji
 - portów

- protokołów.
- Przetwarzanie ruchu sieciowego
 - System musi umożliwiać analizę ruchu sieciowego w sposób rozproszony, z wykorzystaniem urządzeń bezpieczeństwa sieciowego działających w warstwie infrastruktury OT.
 - Analiza ruchu sieciowego musi być realizowana lokalnie na urządzeniach bezpieczeństwa sieciowego poprzez:
 - analizę pakietów,
 - analizę protokołów przemysłowych,
 - analizę anomalii komunikacyjnych.
 - Do centralnego systemu bezpieczeństwa muszą być przekazywane dane przetworzone, obejmujące co najmniej:
 - zdarzenia bezpieczeństwa,
 - metadane komunikacyjne,
 - profile komunikacyjne zasobów,
 - informacje o wykrytych anomaliach.
 - System nie może wymagać przesyłania pełnej kopii ruchu sieciowego do centralnej platformy analitycznej.
- Integracja z urządzeniami sieciowymi i systemami bezpieczeństwa
 - System musi umożliwiać integrację z urządzeniami bezpieczeństwa sieciowego oraz systemami monitoringu infrastruktury zarówno tego samego producenta, jak i innych producentów.
 - System musi umożliwiać:
 - natywną integrację z urządzeniami bezpieczeństwa tego samego producenta, umożliwiającą wymianę danych telemetrycznych, zdarzeń bezpieczeństwa oraz synchronizację polityk bezpieczeństwa,
 - integrację z urządzeniami innych producentów poprzez standardowe mechanizmy wymiany danych, w szczególności:
- Moduł automatycznej analizy incydentów bezpieczeństwa
 - System musi posiadać mechanizm analizy zdarzeń bezpieczeństwa wspierający operatora SOC w procesie klasyfikacji, triage oraz oceny ryzyka incydentów bezpieczeństwa.
 - Mechanizm analityczny musi umożliwiać generowanie raportu analitycznego dla zdarzenia bezpieczeństwa obejmującego co najmniej:
 - syntetyczne podsumowanie zdarzenia (Executive Summary),
 - analizę techniczną zdarzenia,
 - ocenę charakteru zdarzenia (atak, anomalia, zdarzenie informacyjne, brak danych),
 - ocenę poziomu ryzyka i poziomu wiarygodności analizy,
 - identyfikację powiązanych systemów, usług oraz zasobów infrastruktury,
 - mapowanie zdarzeń do technik MITRE ATT&CK dla środowisk Enterprise oraz ICS,

- analizę potencjalnych podatności powiązanych ze zdarzeniem w oparciu o bazę CVE,
 - ocenę zgodności zdarzenia z wymaganiami regulacyjnymi i normatywnymi (np. IEC 62443, ISO 27001, NIS2, KSC),
 - rekomendacje działań operacyjnych dla zespołów SOC,
 - analizę konsekwencji braku reakcji na zdarzenie,
 - końcową klasyfikację zdarzenia.
- Analiza incydentów bezpieczeństwa
 - System musi posiadać mechanizm automatycznej analizy zdarzeń bezpieczeństwa umożliwiający generowanie raportu analitycznego dla wskazanego zasobu (asset) na podstawie zestawu powiązanych zdarzeń.
 - Mechanizm analityczny musi umożliwiać:
 - korelację zdarzeń pochodzących z jednego zasobu lub powiązanych zasobów,
 - analizę kontekstu komunikacji sieciowej,
 - ocenę charakteru zdarzeń (atak / anomalia / zdarzenie informacyjne / działanie polityki bezpieczeństwa),
 - analizę zachowania zasobu w odniesieniu do jego profilu komunikacyjnego,
 - identyfikację usług sieciowych, protokołów oraz typów komunikacji,
 - identyfikację usług publicznych lub znanych dostawców infrastruktury
- Raportowanie analityczne
 - System musi umożliwiać automatyczne generowanie raportu analitycznego obejmującego co najmniej:
 - ocenę poziomu pilności zdarzenia (SOC triage),
 - syntetyczne podsumowanie analizy (Executive Summary),
 - analizę techniczną zdarzeń,
 - ocenę charakteru zdarzenia,
 - mapowanie zdarzeń do MITRE ATT&CK,
 - analizę potencjalnych podatności (CVE),
 - analizę wpływu na zgodność regulacyjną (IEC 62443, ISO 27001, NIS2, KSC),
 - rekomendacje działań dla zespołu SOC,
 - ocenę konsekwencji braku reakcji,
 - końcową klasyfikację zdarzenia.

2.5. System / moduł korelacji

- System musi stanowić platformę korelacji umożliwiającą:
 - orkiestrację procesów reagowania na incydenty,
 - automatyzację działań operacyjnych,
 - korelację zdarzeń z wielu źródeł,
 - realizację reakcji w środowisku IT i OT.
- System musi posiadać:
 - centralny silnik korelacyjny (event processing engine),

- graficzny silnik playbooków (workflow engine),
 - moduł zarządzania alarmami (incident lifecycle),
 - warstwę integracyjną z urządzeniami bezpieczeństwa dostarczonymi w ramach Zamówienia.
- System musi umożliwiać:
 - Tworzenie graficznych playbooków reakcji incydentowej w modelu:
 - event-driven,
 - stateful (utrzymywanie stanu),
 - warunkowym (IF/AND/OR).
 - Budowę wieloetapowych scenariuszy zawierających:
 - filtry zdarzeń,
 - agregację progową (threshold),
 - korelację czasową (time window),
 - warunki logiczne,
 - akcje reakcyjne.
 - Łączenie zdarzeń pochodzących z różnych źródeł (np. IDS, firewall, NDR, monitoring OT).
 - Obsługę sygnałów wejścia/wyjścia między węzłami (signal-based workflow).
- System musi umożliwiać automatyczne:
 - Generowanie alarmów na podstawie warunków korelacyjnych.
 - Agregowanie zdarzeń w jeden incydent.
 - Resetowanie i czyszczenie kontekstu po zakończeniu scenariusza.
 - Dynamiczne przypisywanie poziomu wiarygodności (reliability).
 - Wykonywanie akcji na podstawie:
 - przekroczenia progu zdarzeń,
 - przekroczenia limitu czasowego,
 - spełnienia warunków logicznych.
- System musi realizować:
 - Korelację progową (N zdarzeń w czasie T).
 - Korelację czasową (timeout-based).
 - Korelację wieloźródłową (cross-source).
 - Korelację kontekstową (asset-aware correlation).
 - Grupowanie zdarzeń w ramach jednego incydentu.
 - Mechanizm resetu stanu po spełnieniu warunków.
- System musi zapewniać:
 - Pełny lifecycle alarmu:
 - utworzenie,
 - aktualizacja,
 - rozwiązanie,
 - wyciszenie,
 - zamknięcie.
 - Rejestr linii czasu (timeline).

- Powiązanie alarmu z zasobem i zdarzeniami.
- Klasyfikację poziomu ryzyka.
- Możliwość raportowania i eksportu danych.
- Licencja nie może ograniczać ilości IP, MAC, scenariuszy reakcyjnych

2.6. System typu EDR/XDR

- Architektura systemu
 - System musi być rozwiązaniem klasy EDR (Endpoint Detection and Response) umożliwiającym:
 - monitorowanie zdarzeń bezpieczeństwa na stacjach roboczych i serwerach,
 - detekcję zagrożeń w czasie rzeczywistym,
 - korelację zdarzeń,
 - reakcję na incydenty.
 - System musi składać się z:
 - agentów instalowanych na chronionych hostach,
 - centralnego serwera zarządzającego,
 - silnika analityczno-korelacyjnego,
 - repozytorium logów,
 - interfejsu webowego (GUI).
 - System musi umożliwiać instalację:
 - w środowisku lokalnym (on-premise),
 - w środowisku wirtualnym,
- Obsługiwane systemy operacyjne
 - Agent musi obsługiwać co najmniej:
 - Windows (Server i Workstation),
 - Linux (różne dystrybucje).
 - System musi umożliwiać centralne zarządzanie konfiguracją agentów.
- Funkcjonalności EDR – detekcja
 - System musi zapewniać:
 - Monitoring integralności plików (FIM – File Integrity Monitoring):
 - wykrywanie zmian w plikach systemowych i konfiguracyjnych,
 - wykrywanie zmian w rejestrze Windows,
 - generowanie alertów przy nieautoryzowanych modyfikacjach.
 - Monitoring procesów:
 - rejestrowanie uruchamianych procesów,
 - analiza linii poleceń (command line),
 - wykrywanie podejrzanych procesów (np. PowerShell, WMI, LOLBins).
 - Monitoring aktywności użytkowników:
 - logowania lokalne i zdalne,
 - próby eskalacji uprawnień,
 - zmiany w grupach uprzywilejowanych.
 - Detekcję malware i rootkitów:
 - wbudowany mechanizm rootkit detection,

- integrację z zewnętrznymi silnikami AV (np. ClamAV).
- Detekcję anomalii i ataków zgodnie z MITRE ATT&CK:
 - mapowanie zdarzeń do technik ATT&CK,
 - możliwość generowania raportów według taksonomii MITRE.
- Wykrywanie podatności (Vulnerability Detection):
 - identyfikację zainstalowanego oprogramowania,
 - korelację z bazami CVE,
 - raportowanie podatności.
- Korelacja i analiza
 - System musi posiadać:
 - silnik reguł (rule-based detection),
 - możliwość tworzenia własnych reguł detekcyjnych,
 - możliwość korelacji wielu zdarzeń w jeden incydent.
 - System musi:
 - wspierać analizę logów z różnych źródeł (systemowe, aplikacyjne, sieciowe),
 - umożliwiać integrację z Syslog,
 - umożliwiać integrację z urządzeniami sieciowymi.
- Funkcjonalności Response
 - System musi umożliwiać:
 - Zdalne wykonywanie komend na gościu.
 - Blokowanie adresów IP (np. poprzez integrację z firewall).
 - Automatyczne reakcje (active response) na podstawie zdefiniowanych reguł.
 - Izolację hosta (logicznie – poprzez blokowanie komunikacji).
 - System musi umożliwiać wywoływanie reakcji z poziomu SOAR zintegrowanego z główną konsolą.
- Zarządzanie i raportowanie
 - System musi posiadać:
 - interfejs webowy (dashboard),
 - wyszukiwarkę zdarzeń,
 - możliwość filtrowania po hostach, użytkownikach, czasie, typie zagrożenia.
 - System musi umożliwiać:
 - generowanie raportów PDF/CSV,
 - raporty zgodności (np. PCI-DSS, CIS, ISO 27001),
 - raporty podatności.
 - System musi umożliwiać wielopoziomowe role użytkowników (RBAC).
- Integracje
 - System musi umożliwiać integrację z:
 - SIEM,
 - systemami SOC,
 - systemami zarządzania podatnościami,
 - bazami threat intelligence,

Bezpieczeństwo systemu

2. Komunikacja agent–serwer musi być szyfrowana (TLS).
3. System musi posiadać:
 - mechanizmy uwierzytelniania,
 - role i uprawnienia,
 - logowanie działań administratorów.

Zadanie 34. UTM (Unified Threat Management) Platforma sprzętowa DIN35 - System bezpieczeństwa IPS/IDS, OT Anomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat) , AI Sanitization, AI MGMT, ZBFW

2. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 1 sztuki urządzenia przeznaczonego do ochrony i monitorowania środowisk OT, w postaci platform sprzętowych klasy UTM (Unified Threat Management), przystosowanych do montażu na szynie DIN35, wraz z funkcjonalnościami z zakresu bezpieczeństwa teleinformatycznego, zgodnie z wymaganiami technicznymi i funkcjonalnymi określonymi przez Zamawiającego.

3. Wymagania dotyczące rozwiązania:

2.1. Wymagania ogólne dla urządzeń:

- musi być nowy (nie starszy niż z 4 kwartału 2025 r) i pochodzić z polskiego kanału dystrybucji
- musi posiadać gwarancję i wsparcie producenta na okres nie krótszy niż do 30.06.2026
- producent musi zapewnić czas życia produktu do końca roku 2032 roku. Nie dopuszcza się rozwiązań będących w okresie zakończenia życia (end-of-life) lub zakończenia wsparcia (end-of-support) lub zakończenia sprzedaży (end-of-sale).

2.2. Wymagania ogólne dla urządzeń aktywnych sieci

- Urządzenia montowane na szynę DIN35mm muszą:
 - Być dostarczone z dwoma zasilaczami 230 V / DC 24 V dostosowane mocowo do dostarczanych urządzeń działające w układzie nadmiarowym i uzupełniającym
 - Posiadać strukturę modułarną (nie dopuszcza się sprzętu które posiada chociaż jednego modułu rozszerzeń do którego można dołożyć – po za projektem np. dodatkowy moduł komunikacyjny np. LTE lub WiFi
 - Posiadać aktualny certyfikat IEC 62443 4-2 SL4 akredytowany przez PCA
 - Urządzenia muszą stanowić platformę bezpieczeństwa obok standardowych funkcjonalności urządzeń aktywnych sieci takich jak przełączanie czy routing L3.
 - Być montowane na szynach wysuwanych umożliwiając łatwy dostęp do górnej części urządzenia
 - Muszą posiadać certyfikat FCC Class A, CE, UL

Parametr	Opis / wartość parametru	Ilość
Pamięć RAM	Min. 8 GB	1
Storage	Min. 480 GB	1
Interfejs Szeregowy	Konsola RS232	1
Zasilacze	230 V 5 A – 24 V DC	2
Interfejs 1 Gb/s	RJ45 Ethernet with 2 porty bypass	Minimum 2 pracujące w trybie bypass (utrzymanie łączności w przypadku braku zasilania)
Interfejs 1 Gb/s	SFP 1 Gb/s	Minimum 2 x SFP 1 Gb/s.
Wkładki 1 Gb/s	SFP 1 Gb/s	2 sztuki – parametry: 10 KM 1310 nm SM
Moduł GSM	LTE, antena GSM x 2	1
Uchwyty montażowe	1 komplet dla DIN35	1
Kable zasilające	Min 0,5 m	2

Typ montażu	Szyna DIN35	n/d
Patch cordy	Miedziane CAT6, 1,5 M RJ45	2
Patch cordy	Światłowodowe SC/LC 1,5 m SM PC/APC LC-LC	2
Montaż	Szyna DIN35	n/d
Konsola centralna	Zarządzanie Firewall z poziomu konsoli centralnej zintegrowanej z centralnym systemem SIEM/IDS, pochodząca od tego samego producenta co urządzenie aktywne	n/d
Certyfikaty wymagane	CE, FCC Class A, UL, IEC 62443 4-2 SL4	n/d
Temperatura pracy	Od minus 40 stopni Celsjusza do plus 70 stopni Celsjusza	

2.3. Wymagania dla funkcjonalności systemu pracującego na urządzeniu:

- Routing i przełączanie (L2 / L3)
 - Pełny routing IPv4 i IPv6 (statyczny, dynamiczny, policy-based, VRF).
 - Obsługa protokołów routingu: OSPFv2/v3, BGP, RIP, RIPng, Babel, IS-IS.
 - VRRP – redundancja bramy sieciowej (High Availability).
 - MPLS / VPLS / LDP / RSVP – wsparcie dla sieci operatorskich i segmentacji.

- Policy-Based Routing (PBR) – wybór trasy na podstawie źródła, portu, typu ruchu.
 - Ethernet bridging (L2) – możliwość pracy jako przełącznik (bridge, VLAN, trunk).
 - STP / RSTP – obsługa protokołów zapobiegających pętlom w sieci.
 - 802.1Q VLAN / QinQ – pełne wsparcie dla VLAN i tunelowania VLAN w VLAN.
 - LACP / Bonding / Port-channel – łączenie interfejsów dla redundancji i wydajności.
 - VRF / Route Tables – separacja ruchu i izolacja sieci logicznych.
- Firewall i bezpieczeństwo
 - Stateful Firewall (ZBFW – Zone-Based Firewall) – inspekcja stanu połączeń i przypisanie reguł do stref logicznych.
 - NAT (Source, Destination, Static, Masquerade) – pełna translacja adresów.
 - Policy NAT i Hairpin NAT – elastyczne mapowanie adresów w zależności od kierunku.
 - IPv6 Firewall – osobne polityki bezpieczeństwa dla IPv6.
 - Traffic Filtering na poziomie L2–L4 – filtrowanie pakietów, portów, protokołów.
 - Time-based Rules – polityki bezpieczeństwa zależne od czasu.
 - Conntrack / Helper modules – śledzenie sesji i stanów połączeń.
 - Rate-limiting / DoS protection – ograniczanie przepustowości, ochrona przed floodem.
 - MAC Firewall / ARP Inspection / Static ARP tables – kontrola komunikacji warstwy drugiej.
- VPN i tunelowanie
 - IPsec IKEv1 / IKEv2 – szyfrowane tunele site-to-site i remote access.
 - L2TP, PPTP, OpenVPN, WireGuard – elastyczne protokoły VPN dla użytkowników i urządzeń.
 - GRE / mGRE / VTI / VXLAN / IP-in-IP – tunelowanie ruchu między sieciami (np. SCADA ↔ DMZ).
 - Dynamiczny routing przez VPN (BGP over IPsec) – skalowalność w dużych sieciach.
 - DMVPN V3 – automatyka zestawiania topologii HUB Spoke z zabezpieczeniem IPsec i protokołami routingu wraz z protokołem NHRP
 - SSL VPN / Remote Access – wsparcie dla zdalnego dostępu użytkowników.
- QoS i kontrola ruchu
 - Traffic Shaping / Policing / Queueing (HTB, CBQ, HFSC) – kontrola pasma.
 - Hierarchical QoS (HQoS) – wielopoziomowe kolejkowanie.
 - Traffic Classification (DSCP / CoS / ACL match) – klasyfikacja ruchu na podstawie atrybutów.
 - Bandwidth Management per interface / per VLAN – kontrola przepustowości per-port lub per-sieć.
- Monitoring, logowanie i diagnostyka
 - SNMP v1/v2c/v3 – monitorowanie zewnętrzne.
 - Syslog (lokalny i zdalny) – pełna integracja logów z systemami SIEM/IDS.
 - NetFlow / sFlow / IPFIX – eksport statystyk ruchu do systemów analitycznych.
 - Ping / Traceroute / MTR / Packet Capture (tcpdump) – diagnostyka sieciowa.

- BFD – szybkie wykrywanie awarii tras routingu.
- Interface Counters / Flow statistics – bieżące statystyki ruchu.
- Monitorowanie w trybie inline – analityka DPI oraz IDS realizowana pasywnie w trybie ciągłym na każdym interfejsie aktywnym,
- Mirror Port – możliwość skopiowania ramek z interfejsów źródłowych na interfejs wyjściowy
- Przekierowanie wewnętrzne do systemów analityki – funkcja zautomatyzowana przekierowania ruchu przez wewnętrzny system IPS (w trybie IPS) dla analityki z automatyka ochrony inline
- Analityka anomalii komunikacji sieciowej pomiędzy komponentami
- Behavioral monitoring,
- Profilowanie obiektów logicznych i fizycznych sieci
- Identyfikacja komponentów w danych z ruchu sieciowego
- Analityka czasów transmisji dla komunikacji sesyjnej i niesesyjnej
- Traceability dla podanych parametrów zidentyfikowanych w ruchu sieciowym
- Tryb maintenance dla wyciszenia alertów z profili zgłoszonych do zmiany w środowisku sieciowym
- Thread Detection
- Analityka głęboka protokołów IT i OT w tym Modbus TCP, Goose, Profinet, Ethernet/IP, EtherCat, S-BUS, Step7, IEC 60870-5-104
- Diagnostyka protokołów OT
- Diagnostyka protokołów IT
- Wbudowany system traceability dla monitorowania głębokich danych do poziomu nastaw i wartości np. rejestrów
- Zarządzanie i automatyzacja
 - CLI / SSH / API / RESTCONF / NETCONF – wielowarstwowe zarządzanie.
 - Konfiguracja CLI w stylu Cisco / Juniper – logiczne drzewo konfiguracji.
 - Atomic commits / rollback / diff – bezpieczne zmiany i cofanie konfiguracji.
 - Scheduled tasks / cron / event-driven scripts – automatyzacja procesów.
 - Ansible / Salt / Terraform ready – zgodność z narzędziami DevOps.
 - Zarządzanie użytkownikami / RADIUS / TACACS+ / LDAP – kontrola dostępu administracyjnego.
 - Backup / restore / config versioning – bezpieczeństwo konfiguracji.
 - Zarządzanie Firewall – wymagane jest również zarządzanie z poziomu konsoli centralnej

2.4. IDS/IPS

- **Detekcja, analiza i blokowanie zagrożeń sieciowych w czasie rzeczywistym.**
 - Analiza i inspekcja ruchu sieciowego (Deep Packet Inspection – DPI)
 - Pełna inspekcja pakietów na poziomie L2–L7 w czasie rzeczywistym.
 - Analiza protokołów przemysłowych (Modbus, DNP3, IEC 60870-5-104, PROFINET, BACnet, OPC UA itp.).

- Wykrywanie anomalii w komunikacji sterowników PLC, HMI i urządzeń przemysłowych.
- Rozpoznawanie struktur poleceń, zmiennych procesowych i komunikacji SCADA.
- Detekcja zagrożeń (Intrusion Detection System – IDS)
 - Wykrywanie prób włamań, skanowania portów, exploitów, ataków DoS/DDoS i naruszeń polityk sieciowych.
 - Identyfikacja złośliwego oprogramowania, beaconingu i nieautoryzowanych połączeń C2 (Command & Control).
 - Korelacja zdarzeń z regułami IDS Rules oraz regułami zespołu MDR i CTI.
 - Generowanie alertów i przekazywanie ich do systemu SIEM/IDS.
- Blokowanie zagrożeń (Intrusion Prevention System – IPS)
 - Dynamiczne blokowanie pakietów i sesji zgodnie z regułami bezpieczeństwa.
 - Automatyczne odcinanie źródeł ataków, modyfikacja polityk firewallowych w czasie rzeczywistym.
 - Współpraca z modułem firewall (ZBFW) i komponentami SIEM/IDS w celu natychmiastowej reakcji.
 - Minimalny wpływ na opóźnienia i przepustowość ruchu sieciowego (low-latency design).
- Analiza sygnatur i anomalii
 - Wykorzystanie sygnatur znanych ataków oraz mechanizmów heurystycznych i statystycznych.
 - Wykrywanie anomalii w zachowaniach urządzeń i użytkowników (np. nagłe wzrosty ruchu, zmiana portów, niezgodność protokołów).
 - Wsparcie dla analizy behawioralnej w połączeniu z modułami CTI i MDR.
 - Aktualizacje baz reguł bezpieczeństwa w sposób automatyczny i kontrolowany.
- Integracja z systemami analitycznymi i korelacyjnymi
 - Wysyłanie logów i alertów do systemów SIEM, SOC, MDR.
 - Normalizacja danych i mapowanie zdarzeń do frameworków MITRE ATT&CK i IEC 62443.
 - Współpraca z bazami danych CTI w celu identyfikacji źródeł zagrożeń i kampanii APT.
 - Eksport danych w formatach EVE JSON, Syslog, PCAP i NetFlow.
- Wsparcie inspekcji w sieciach OT
 - Zoptymalizowane reguły detekcji dla środowisk przemysłowych.
 - Tryb „passive monitoring” bez ingerencji w ruch procesowy (dla systemów krytycznych).
 - Tryb „inline” z prewencyjnym blokowaniem ataków przy zachowaniu zgodności z IEC 62443-3-3.
 - Pełna widoczność komunikacji pomiędzy segmentami IT a OT.

- Mechanizmy automatyzacji i korelacji
 - Automatyczne przekazywanie alertów do modułów reakcji MDR.
 - Aktywacja polityk obronnych w firewallu .
 - Dynamiczne uczenie się ruchu sieciowego (profilowanie).
 - Możliwość tworzenia własnych reguł i skryptów reakcji w środowisku SIEM/IDS.
- Raportowanie i wizualizacja
 - Raporty incydentów bezpieczeństwa, trendów i statystyk detekcji.
 - Graficzne przedstawienie ruchu sieciowego i źródeł zagrożeń w panelu SIEM/IDS.
 - Eksport alertów i logów do systemów zewnętrznych w formacie JSON, CSV, Syslog.
 - Możliwość integracji z pulpitemi centralnego SIEM/IDS .
- Dodatkowe moduły
 - DHCP server/relay/client, DNS server/forwarder, NTP, HTTP proxy, NetBIOS relay.
 - Dynamic DNS, Static Hosts, Name-resolution cache.
 - Multicast routing (PIM/IGMP).
 - IPv6 autoconfiguration / router advertisement (RA).
 - System High Availability (VRRP, Sync) – redundancja i przełączenie awaryjne.
 - Zarządzanie certyfikatami SSL / PKI – obsługa CA, kluczy i certyfikatów.
- Dodatkowe cechy
 - Rolling Release – aktualizacje bezpieczeństwa w cyklu ciągłym.
 - Integracja z Docker / LXC / KVM – uruchamianie usług w kontenerach.
 - Obsługa Netfilter nftables / eBPF – nowoczesne mechanizmy filtrowania.
 - Gwarancja 24 miesiące

Zadanie 35. Usługa Private APN

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie 4 usług Private APN, przeznaczonej do realizacji bezpiecznej i wydzielonej transmisji danych pomiędzy urządzeniami a infrastrukturą teleinformatyczną Zamawiającego, zgodnie z wymaganiami technicznymi i funkcjonalnymi określonymi w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania

2.1. Wymagania bezpieczeństwa dla sieci APN

- **Zakres funkcjonalny**
 - W ramach realizacji usługi transmisji danych w oparciu o sieć APN operatora telekomunikacyjnego Wykonawca zobowiązany jest zapewnić mechanizmy

- bezpieczeństwa umożliwiające ochronę oraz monitoring komunikacji pomiędzy urządzeniami infrastruktury Zamawiającego.
- Usługa APN musi umożliwiać integrację z systemami cyberbezpieczeństwa Zamawiającego oraz zapewniać możliwość automatycznego monitorowania komunikacji w ramach infrastruktury telekomunikacyjnej.
 - **Monitoring bezpieczeństwa komunikacji**
 - Infrastruktura realizująca usługę APN musi umożliwiać prowadzenie automatycznego monitoringu bezpieczeństwa komunikacji w trybie ciągłym (SOC monitoring).
 - Monitoring musi obejmować co najmniej:
 - identyfikację urządzeń komunikujących się w sieci APN,
 - analizę kierunków komunikacji pomiędzy zasobami infrastruktury,
 - identyfikację anomalii komunikacyjnych,
 - wykrywanie prób nieautoryzowanego dostępu do infrastruktury Zamawiającego,
 - analizę zdarzeń bezpieczeństwa generowanych w ramach komunikacji APN.
 - **Integracja z systemem cyberbezpieczeństwa Zamawiającego**
 - System realizujący monitoring bezpieczeństwa komunikacji APN musi umożliwiać przekazywanie zdarzeń bezpieczeństwa do systemu cyberbezpieczeństwa Zamawiającego.
 - W szczególności wymagane jest:
 - automatyczne przekazywanie alarmów bezpieczeństwa,
 - przekazywanie zdarzeń związanych z anomaliami komunikacyjnymi,
 - przekazywanie zdarzeń związanych z próbami nieautoryzowanego dostępu.
 - Integracja musi odbywać się w sposób umożliwiający automatyczne przetwarzanie zdarzeń przez system cyberbezpieczeństwa Zamawiającego.
 - **Ochrona kryptograficzna komunikacji**
 - Komunikacja realizowana w ramach infrastruktury APN musi być chroniona z wykorzystaniem mechanizmów kryptograficznych zapewniających poufność oraz integralność transmisji danych.
 - W szczególności wymagane jest stosowanie mechanizmów:
 - szyfrowania transmisji danych,
 - uwierzytelniania urządzeń komunikujących się w sieci,
 - ochrony integralności przesyłanych danych.
 - Mechanizmy kryptograficzne muszą zapewniać ochronę komunikacji pomiędzy urządzeniami Zamawiającego niezależnie od infrastruktury operatora telekomunikacyjnego.
 - **Niezależność systemu cyberbezpieczeństwa**
 - System monitorowania bezpieczeństwa komunikacji musi być realizowany w sposób umożliwiający analizę zdarzeń bezpieczeństwa w systemie cyberbezpieczeństwa Zamawiającego, niezależnie od infrastruktury operatora telekomunikacyjnego.
 - Zamawiający musi posiadać możliwość niezależnej analizy zdarzeń bezpieczeństwa związanych z komunikacją w sieci APN.
 - **Wymagania dotyczące zdarzeń bezpieczeństwa**

- System monitorowania komunikacji APN musi generować zdarzenia bezpieczeństwa obejmujące co najmniej:
 - wykrycie nieautoryzowanych urządzeń w sieci,
 - próby nawiązania nieautoryzowanych połączeń,
 - anomalie w komunikacji sieciowej,
 - próby naruszenia integralności komunikacji.
- Zdarzenia bezpieczeństwa muszą być przekazywane do systemu cyberbezpieczeństwa Zamawiającego w sposób automatyczny.
- **Analiza i inspekcja protokołów przemysłowych**
- Infrastruktura realizująca usługę transmisji danych w sieci APN musi umożliwiać analizę komunikacji pomiędzy urządzeniami infrastruktury przemysłowej Zamawiającego.
- System monitorowania bezpieczeństwa musi umożliwiać identyfikację oraz analizę protokołów komunikacyjnych wykorzystywanych w infrastrukturze OT/ICS/IloT.
- W szczególności wymagane jest zapewnienie możliwości analizy protokołów przemysłowych obejmujących między innymi:
 - Modbus
 - DNP3
 - IEC 60870-5-104
 - IEC 61850
 - S7
 - OPC
 - inne protokoły wykorzystywane w infrastrukturze przemysłowej Zamawiającego.
- Analiza musi obejmować co najmniej:
 - identyfikację urządzeń komunikujących się z wykorzystaniem protokołów przemysłowych,
 - identyfikację relacji komunikacyjnych pomiędzy urządzeniami,
 - identyfikację funkcji oraz operacji wykonywanych w ramach komunikacji przemysłowej,
 - identyfikację nieautoryzowanych lub nietypowych operacji komunikacyjnych.
- **Inspekcja komunikacji w tunelach transmisyjnych**
- System bezpieczeństwa infrastruktury Zamawiającego musi umożliwiać analizę oraz inspekcję komunikacji realizowanej pomiędzy urządzeniami Zamawiającego w ramach sieci APN operatora telekomunikacyjnego.
- Analiza komunikacji musi być realizowana w sposób umożliwiający identyfikację zdarzeń bezpieczeństwa w komunikacji pomiędzy urządzeniami infrastruktury przemysłowej niezależnie od infrastruktury operatora telekomunikacyjnego.
- System musi umożliwiać:
 - analizę komunikacji przemysłowej realizowanej w tunelach transmisyjnych,
 - identyfikację nieautoryzowanych poleceń sterujących,
 - identyfikację prób manipulacji komunikacją przemysłową,
 - identyfikację anomalii w komunikacji pomiędzy urządzeniami.
- **Generowanie zdarzeń bezpieczeństwa dla komunikacji OT**

- System monitorowania komunikacji APN musi generować zdarzenia bezpieczeństwa w przypadku wykrycia:
 - nieautoryzowanych poleceń sterujących w protokołach przemysłowych,
 - nieautoryzowanej komunikacji pomiędzy urządzeniami infrastruktury,
 - prób manipulacji komunikacją przemysłową,
 - anomalii komunikacyjnych w relacjach pomiędzy urządzeniami.
- Zdarzenia bezpieczeństwa muszą być przekazywane do systemu cyberbezpieczeństwa Zamawiającego w sposób automatyczny.
- **Integracja z systemem SOC**
- System monitorowania komunikacji APN musi umożliwiać integrację z systemem Security Operations Center (SOC) Wykonawcy w ramach dostawy usługi SOC / MDR.
- W szczególności wymagane jest:
 - przekazywanie zdarzeń bezpieczeństwa w czasie rzeczywistym,
 - przekazywanie alarmów bezpieczeństwa,
 - przekazywanie danych umożliwiających analizę incydentów bezpieczeństwa.
- Integracja musi umożliwiać automatyczne przetwarzanie zdarzeń bezpieczeństwa przez system cyberbezpieczeństwa Zamawiającego.

Zadanie 36. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa 2 sztuki urządzenia typu UPS, przeznaczonych do zapewnienia awaryjnego zasilania dla urządzeń i systemów bezpieczeństwa teleinformatycznego, zgodnych z wymaganiami technicznymi określonymi w dokumentacji postępowania.

2. Wymagania dotyczące rozwiązania

2.1. Parametry mocy i wydajności:

- Moc pozorna: 2000 VA
- Moc rzeczywista: 1800 W
- Współczynnik mocy (pf): 0,9
- Topologia: Online (podwójna konwersja)
- Czas przełączenia na baterię: 0 ms
- Współczynnik szczytu: 3:1

2.2. Parametry wejściowe:

- Napięcie znamionowe: 200/208/220/230/240 V
- Tolerancja napięcia prostownika: 160 V – 276 V (regulacja programowa 120-276 V z obniżeniem wartości znamionowej)
- Częstotliwość znamionowa: 50/60 Hz (autodetekcja)
- Tolerancja częstotliwości: 40 – 70 Hz
- Typ gniazda wejściowego: IEC C14 10A

2.3. Parametry wyjściowe:

- Napięcie znamionowe wyjściowe: 200/208/220/230/240 V (do wyboru przez użytkownika)
- Częstotliwość wyjściowa: 50/60 Hz
- Kształt napięcia: Sinusoidalny
- Liczba i typ gniazd wyjściowych: 6 x IEC C13

2.4. Baterie i czas podtrzymania:

- Czas podtrzymania: Minimum 4 minuty dla 100% obciążenia (przy $pf=0,9$)
- Baterie wymieniane przez użytkownika „na gorąco” (Hot-swap)
- Okresowy automatyczny test baterii
- Ochrona przed przeładowaniem (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
- Ochrona przed głębokim rozładowaniem
- Możliwość uruchomienia bez napięcia w sieci („zimny start”)

2.5. Komunikacja i zarządzanie:

- Interfejsy: USB, RS232 DB-9 żeński (HID), styki przekaźnikowe, miniport wyłącznik ON/OFF
- Slot rozszerzeń: Na kartę komunikacyjną SNMP/Ethernet
- Panel sterowania: Wyświetlacz LCD z menu w języku polskim
- Elementy panelu: Poziomy rząd przycisków sterowania oraz poziomy rząd wskaźników stanu: zasilanie z sieci (zielony), tryb bateryjny (żółty), usterka (czerwony)
- Przyciski sterujące: Escape (anulowanie), Przyciski funkcyjne (góra/dół), Enter (potwierdzający), Przycisk ON/OFF
- Sygnalizacja akustyczna: Alarmy dla stanów: Awaria, Niski stan naładowania baterii, Przeciążenie, Serwis

2.6. Konstrukcja i środowisko:

- Typ obudowy: Rack 2U (maksymalna wysokość urządzenia 2U)
- Poziom hałasu w odl. 1m: Do 50 dBA dla pracy normalnej

2.7. Certyfikaty i gwarancja:

- Znaki bezpieczeństwa: CE, CB Report, EN IEC 62040-1:2019, IEC 62040-2:2016, EN IEC 62040-2:2006
- Gwarancja producenta: 24 miesiące

2.8. Wyposażenie standardowe:

- Jednostka UPS, instrukcja obsługi, instrukcja bezpieczeństwa
- 1 x kabel komunikacyjny USB
- 2 x kable wyjściowe IEC 10A
- 2 x szyny do montażu w szafie 19 cali

2.9. Wymagania formalne:

Wszystkie elementy mają być nowe, nieużywane i wyprodukowane przez producenta UPS-Do oferty należy załączyć oświadczenie producenta potwierdzające ten fakt oraz informację o pochodzeniu sprzętu z oficjalnego kanału dystrybucji na rynek polski.

Zadanie 37. Usługa inwentaryzacji aktywów teleinformatycznych OT.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usługi inwentaryzacji aktywów teleinformatycznych w obszarach OT. Celem realizacji usługi jest przeprowadzenie analizy istniejącej dokumentacji oraz instalacji obiektowych, w celu opracowania materiałów i produktów wstępnych niezbędnych do rozpoczęcia pierwszych etapów projektowania.

2. Wymagania dotyczące usługi

2.5. Zakres ogólny

- Wprowadzenie i wstępne spotkanie robocze

- Cel: Uzyskanie wspólnej wizji realizacji prac fazy wraz z ustaleniem wytycznych i zakresu merytorycznego prac. Przekazanie dokumentacji. Omówienie dokumentacji i jej zakresu merytorycznego.
- Przygotowanie produktów wstępnych procesu inwentaryzacji (karty inwentaryzacji)
- Miejsce realizacji prac fazy
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY

2.6. Inwentaryzacja obiektów fizycznych w formie Audytu - Zakres ogólny

- Wprowadzenie i wstępne spotkanie robocze
 - Cel: Ustalenie wytycznych i zakresu merytorycznego prac. Akceptacja planu audytu fizycznego na obiekcie.
 - Zmapowanie zapisów dokumentacji ze środowiskiem fizycznym
 - Przegląd procesów głównych i wspomagających, zadań jednostki, czynności stanowiskowych, rodzajów informacji (pod kątem cyberbezpieczeństwa), u Zamawiającego.
 - Przegląd infrastruktury OT w stopniu wymaganym do przeprowadzenia analiz.
 - Wywiady z pracownikami zakładu
 - Konsultacje z kadrą zarządzającą obszarami merytorycznymi
 - Miejsce realizacji prac fazy
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY
- Inwentaryzacja musi być wykonana pod kątem późniejszego projektowania koncepcyjnego
- Zakres ogólny
 - Obszary podlegające opracowaniu:
 - Systemy skomputeryzowane
 - Komunikacja sieciowa
 - Monitoring systemów i transmisji danych
 - Interfejsy systemowe
 - Miejsce realizacji prac
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO oraz
 - Biuro WYKONAWCY

2.7. DOKUMENTACJA - PRODUKTY POSZCZEGÓLNYCH ETAPÓW

- Produkt
 - Dokumentacja inwentaryzacyjna i analityczna.
- Format
 - Pisemny, drukowany oraz w edytowalnej formie elektronicznej (format pliku do wyboru docx, odt, vpp).
- Sposób dostarczenia produktu
 - Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
 - Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego
- Miejsce realizacji prac

- Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO lub
- Biuro WYKONAWCY
- Inwentaryzacja obiektów fizycznych w formie Audytu
 - Obszary podlegające opracowaniu
 - Systemy skomputeryzowane
 - Komunikacja
 - Interfejsy systemowe
 - Opis projektowanych systemów OT
 - Wytyczne i wymagania producentów poszczególnym komponentów głównych
 - Format
 - Pisemny, w edytowalnej formie elektronicznej (format pliku docx, odt, vpp).
 - Mapa połączeń wykonana zgodnie z notacją Archimate 2.0 lub nowszą
 - Sposób dostarczenia produktu
 - Osobiście przez członka zespołu wykonawczego ze strony WYKONAWCY.
 - Podczas procesu dostarczenia produktu odbywa się transfer wiedzy w postaci prezentacji wyników analiz i dyskusji z członkami zespołu wykonawczego ZAMAWIAJĄCEGO produktów projektu
 - Miejsce realizacji prac
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY

2.8. Zakres szczegółowy inwentaryzacji

- Inwentaryzacja ma być wykonana do poziomu urządzeń aktywnych systemów AKPiA
- Dokumentacja inwentaryzacyjna ma zawierać:
 - Topologię logiczną sieci warstwy 2
 - Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
 - Eksport do wektorowego PDF
 - Topologia ma zawierać urządzenia ze źródłowymi adresami MAC i wskazaniem portu fizycznego urządzeń sąsiedzkich (np. komputer <-> przełącznik)
 - Topologia ma być ograniczona do punk tu styku z operatorami zewnętrznymi
 - Topologię logiczną sieci warstwy 3
 - Forma graficzna w dowolnym narzędziu pod warunkiem dostarczenie narzędzia do odczytu
 - Eksport do wektorowego PDF
 - Topologia ma zawierać urządzenia ze źródłowymi adresami MAC i wskazaniem portu fizycznego urządzeń sąsiedzkich (np. komputer <-> przełącznik)
 - Topologia ma być ograniczona do punk tu styku z operatorami zewnętrznymi
 - Mapę komunikacji – oznaczenie obiektów, które wymieniają między sobą dane
 - Forma tabelaryczna z oznaczeniem MAC oraz IPv4 źródła i przeznaczenia. W przypadku routingu oznaczyć MAC interfejsu wyjściowego routera jako adres przypisany do IP źródłowego. Wykazać w tabeli powiązanie IP do wielu adresów

- MAC (jeden sprzętowy źródła oraz wszystkie adresy MAC interfejsów wyjściowych routerów w całej ścieżce komunikacyjnej do miejsca docelowego).
- Ustawienia reguł Firewalli
 - Forma tabelaryczna w formacie xlsx lub zgodnym
 - Ujęcie urządzenia, wirtualizacji jeśli istnieje, zapisu reguły, status (aktywna lub nie aktywna) efekt działania,
 - Listy komponentów
 - Forma tabelaryczna w formacie xlsx lub zgodnym
 - Zestawienie musi zawierać minimum, model, lokalizacja, miejsce montażu, numer seryjny lub numer inwentarzowy (jeżeli urządzenie wymaga demontażu – nie dokonujemy tej czynności a numery seryjne lub model pozostawiamy niewypełnione) adres MAC, adres IP, przypisanie do systemu dziedzicznego, właściciel systemu (osoba lub osoby odpowiedzialne za działanie komponentu)
 - Ustawienia zasad dostępu do zasobów do poziomu stacji roboczych i użytkowników
 - Forma tabelaryczna w formacie xlsx lub zgodnym

Wylistowanie użytkowników oraz zasobów sieciowych wraz z przypisaniem do komponentu (jeśli dotyczy) oraz systemu docelowego do poziomu adresu IPv4

Zadanie 38. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji OT/ICS/IoT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przygotowanie projektu rozwiązania z zakresu bezpieczeństwa dla środowisk OT/ICS/IoT, obejmującego dobór urządzeń, oprogramowania oraz usług niezbędnych do wdrożenia i eksploatacji systemu, zgodnie z wymaganiami technicznymi i funkcjonalnymi określonymi przez Zamawiającego.

2. Wymagania dotyczące usługi

2.1. WYMAGANIA WSTĘPNE

- Projekt, stanowiący przedmiot niniejszego OPZ, nie obejmuje rekonfiguracji istniejącego środowiska teleinformatycznego czy automatyki przemysłowej, dostaw sprzętu, oprogramowania czy usług z tymi dostawami związanych.
- Projekt, stanowiący przedmiot niniejszego OPZ, nie obejmuje rekonfiguracji istniejącego środowiska teleinformatycznego czy automatyki przemysłowej, dostaw sprzętu, oprogramowania czy usług z tymi dostawami związanych.

- Realizacja prac projektowych będzie bazowała m.in. na: Prince 2, ISO/IEC 27001, ISO/IEC 27002, C-HAZOP, Ustawie o ochronie danych osobowych, ISO/IEC TR 27002, CPwE, IEC 62443, Ustawie o Krajowym Systemie Cyberbezpieczeństwa – dla dostarczonych rozwiązań
- Metodyki dostarczenia produktów specjalistycznych są dobierane w zależności od skali i zakresu merytorycznego. Notacja dla dokumentacji procesowej – Archimate 3.0 lub BPMN 2.0
- Przebieg realizacji całości zamówienia zakończony przekazaniem dokumentacji projektu wykonawczego dla rozwiązań bezpieczeństwa i monitorowania systemów OT, została ujęta i przedstawiona w Harmonogramie ogólnym poniżej.

2.2. Projektowanie koncepcyjne – przygotowanie projektu koncepcyjnego (zwanego dalej KONCEPCJĄ) - realizacja zatwierdzonego Planu Projektowania - Zakres ogólny

- Przygotowanie projektu koncepcyjnego dla procesowych i algorytmicznych, celem wykazania poziomu zgodności z założeniami i wymaganiami przez ZAMAWIAJĄCEGO. (porównanie wyników inwentaryzacji i koncepcji wstępnej, uzyskanie informacji o potencjalnych rozbieżnościach celem ich uzupełnienia lub modyfikacji koncepcji)
- Obszary podlegające opracowaniu:
 - Systemy skomputeryzowane
 - Warstwa sterowania i automatyki
 - Warstwa manufacturing (zgodne z CPwE)
 - Przemysłowa komunikacja sieciowa
 - Monitoring systemów i transmisji danych
 - Interfejsy systemowe
 - Wytyczne i wymagania producentów poszczególnym komponentów głównych
- Miejsce realizacji prac
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY

2.3. Realizacja procesu projektowania wykonawczego – Wytworzenie projektu Wykonawczego - Zakres ogólny

- Przygotowanie projektu wykonawczego dla ustalonych w KONCEPCJI rozwiązań
- Obszary podlegające fazie
 - Specyfikacja funkcjonalna
 - Specyfikacja projektowa
 - System cyberbezpieczeństwa
 - Instalacja
 - Procesy eksploatacyjne
 - Testy odbiorowe
- Miejsce realizacji prac
 - Miejsce eksploatacji systemów u ZAMAWIAJĄCEGO
 - Biuro WYKONAWCY

2.4. Projekt koncepcyjny

- Projekt koncepcyjny powinien opisywać wymagane przez ZAMAWIAJĄCEGO zakres i formułę działania systemu na poziomie opracowania fizycznego, elektro-mechanicznego

(jeśli dotyczy) oraz topologii L1 do L3 w odniesieniu do modelu OSI, topologię logiczną aplikacji i powinny być oparte na udokumentowanej ocenie ryzyka i wpływu systemu komputerowego. Dokument KONCEPCJI musi zawierać scenariusz użycia danego rozwiązania ukazującego poglądowy sposób pracy operatorów w ramach dostarczanego rozwiązania. Wymagania użytkowników powinny być identyfikowalne w całym cyklu życia systemu komputerowego.

- Scenariusz może być przedstawiony w formie szkolenia stanowiskowego
- Wymaganiem zamawiającego jest pełna wizualizacja zdarzeń i możliwość reakcji na zagrożenie z jednego, centralnego systemu zarządzania widocznością i bezpieczeństwem.
- Wszystkie dane źródłowe: ruch sieci, logi i inne podłączane źródła zarówno z systemów chmurowych czy lokalnych muszą być kolekcjonowane przez system centralny, normalizowany, wizualizowany i musi zapewnić pełną widoczność.

2.5. Wymagana zawartość dokumentu projektowego.

- Wymaga się aby projekt koncepcyjny zawierał niewyłącznie opracowanie poniższych obszarów:
 - Wymogi operacyjne
 - Wymagania funkcjonalne
 - Wymagania dotyczące danych
 - Wymagania techniczne
 - Wymagania dotyczące interfejsu
 - Wymagania środowiskowe
 - Wymagania dostępności
 - Wymogi bezpieczeństwa
 - Wymagania w zakresie utrzymania
 - Opis ograniczeń dla rozwiązania
 - Wymagania dotyczące cyklu życia
 - Opis testów odbiorowych

2.6. WYKONANIE RAPORTU ROZBIEŻNOŚCI

- Raport rozbieżności należy wykonać poprzez porównanie projektu koncepcyjnego oraz wyników przeprowadzonej inwentaryzacji.
- Forma raportu musi być pisemna i musi zawierać informację o różnicach pomiędzy zaakceptowaną przez ZAMAWIAJĄCEGO KONCEPCJĄ a istniejącymi zasobami, które można wykorzystać do realizacji i wdrożenia rozwiązań projektowanych w Projekcie Wykonawczym .
- Raport musi obejmować analogiczny obszar merytoryczny jak projekt koncepcyjny.

2.7. WYKONANIE PROJEKTU WYKONAWCZEGO

- Projekt wykonawczy musi opisywać wymagane przez użytkownika funkcje systemu/rozwiązania, bazując na zaakceptowanym projekcie koncepcyjnym i musi być oparty na udokumentowanej ocenie ryzyka i wpływu. Wymagania użytkowników powinny być identyfikowalne w całym cyklu życia systemu
- Projekt musi spełniać wymagania następujących norm i dobrych praktyk:

- IEC61850
- IEC 62443 w zakresie segmentacji i kontroli sieci
- ISO 27001
- CPwE

Zadanie 39. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source OT/ICS/IloT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wdrożenie urządzeń, oprogramowania oraz rozwiązań z zakresu bezpieczeństwa w środowiskach OT, ICS oraz IloT, w tym również rozwiązań typu open source, a także przeprowadzenie czynności odbiorowych, zgodnie z wymaganiami Zamawiającego. Wdrożenie musi zostać zrealizowane na podstawie uprzednio zaakceptowanego Projektu Wykonawczego.

2. Wymagania dotyczące usługi wdrożenia

2.1. WYMAGANIA WSTĘPNE

- Faza realizacji prac wdrożeniowych, stanowiący przedmiot niniejszego OPZ , ale nie obejmuje rekonfiguracji istniejącego środowiska teleinformatycznego czy automatyki przemysłowej, dostaw sprzętu, oprogramowania czy usług z tymi dostawami związanych.
- Realizacja prac projektowych będzie bazowała m.in. na: Prince 2, ISO/IEC 27001, ISO/IEC 27002, C-HAZOP, Ustawie o ochronie danych osobowych, ISO/IEC TR 27002, CPwE, IEC 62443, Ustawie o Krajowym Systemie Cyberbezpieczeństwa
- Metodyki dostarczenia produktów specjalistycznych są dobierane w zależności od skali i zakresu merytorycznego. Notacja dla dokumentacji procesowej – Archimate 3.0 lub BPMN 2.0 lub w systemie standardu CAD
- Przebieg realizacji całości zamówienia musi być zakończony przekazaniem dokumentacji powykonawczej dla rozwiązań bezpieczeństwa i monitorowania systemów OT
 - Wymaganiem Zamawiającego jest wizualizacja zdarzeń i możliwość reakcji na zagrożenie z jednego, centralnego systemu zarządzania widocznością i bezpieczeństwem.
 - Dane źródłowe: ruch sieci, logi i inne podłączane źródła być kolekcjonowane przez system centralny, normalizowany, wizualizowany i musi zapewnić pełną widoczność.
 - Wykonawca bierze odpowiedzialność za zaprojektowanie i późniejsze działanie systemu w formie zintegrowanej.

- Nie dopuszcza się niezależnych systemów, które będą wymagały, dla uzyskania widoczności danych, logowania się na różne systemy i ich interfejsy.
- Dopuszcza się stosowanie niezależnych dostępów i interfejsów celem zarządzania i wprowadzania zmian w systemie i zarządzanych komponentach podłączonych do danego systemu. Tym samym, szczegółowe zarządzanie może odbywać się na poziomie poszczególnych komponentów całości rozwiązania.
- Wymaganiem jest aby urządzenia OT oraz system centralny pochodziły od tego samego producenta i posiadały Certyfikat IEC 62443 4-2 na poziomie SL4 akredytowany przez PCA lub ISA.
- Urządzenia aktywne sieci zarówno na szynę DIN jak i Rack 9" muszą minimum posiadać certyfikaty CE, FCC Class A, UL lub równoważne, celem upewnienia się, że nadają się do zastosowań w Automatyce Przemysłowej i systemach AKPiA.
- Systemy i produkty podlegające wdrożeniu w środowisku Zamawiającego.
 - Komplementarny system komunikacyjny i cyberbezpieczeństwa OT oparty o dostarczone urządzenia przez Wykonawcę
 - Urządzenie będące jednocześnie (przełącznikiem, routerem, FW i urządzeniem diagnostycznym) –z pełną ochroną i monitorowaniem na platformie sprzętowej rack 19" z systemem bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)
 - Urządzenia będące jednocześnie (przełącznikami, routerami, FW i urządzeniami diagnostycznymi) –z pełną ochroną i monitorowaniem na platformie sprzętowej DIN35 z systemem bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat)
 - Oprogramowanie platformowe - Zintegrowany System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat), SIEM, , AKPiA RSDT, , XDR, NDR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT
 - UTM (Unified Threat Management) - Platforma sprzętowa DIN35 - System bezpieczeństwa IPS/IDS, OT Anomaly Detection, threat detection, data traceability controll, SDN, anti DDOS, anti APT (Advanced Persistent Threat) , AI Sanitization, AI MGMT, ZBFW
 - Usługa Private APN – z kartami SIM - oparta o usługę dostarczoną przez Wykonawcę. Bezpieczeństwo transmisji musi być zapewniane przez Wykonawcę poprzez monitorowanie ruchu przez SOC i własne systemy cyberbezpieczeństwa zlokalizowane u Wykonawcy. SOC Wykonawcy musi legitymować się certyfikacją akredytowaną przez PCA w zakresie minimum ISO 27001 oraz ISO 9001. Dopuszcza się konsorcja lub podwykonawstwo w którym Wykonawca bierze odpowiedzialność za działanie usługi APN.
- Wdrożenie:
 - Wdrożenie ma być wykonane zgodnie z obowiązującymi przepisami BHP. W szczególności wymaga się od Wykonawcy zapewnienia osób wykonujących pracę

- w miejscach wymagających odpowiednich dopuszczeń z odpowiednimi uprawnieniami np. D1 i/lub E1.
- Prace montażowe i uruchomieniowe muszą być uzgodnione z Zamawiającym.
 - Każde prace modyfikujące jakiegokolwiek obszary w strefach OT muszą być odrębnie zatwierdzone przez Zamawiającego
 - Wszelkie zatrzymania lub odstawienia procesu muszą być poprzedzone wydaniem zgody Zamawiającego.
 - Samowolne działania Wykonawcy, które spowodują zatrzymanie, lub odstawienie procesu technologicznego będą podstawą do wniesienia roszczeń za uczynione szkody.
 - Zachowanie na terenie Zamawiającego niezgodnie z zasadami BHP spowoduje natychmiastowe usunięcie przedstawicieli Wykonawcy co nie będzie skutkowało przesunięciem terminu realizacji Zamówienia.
 - Wdrożenie musi zakończyć się wytworzeniem dokumentacji Powykonawczej uwzględniającej
 - Instrukcje dla wdrażanych urządzeń i systemów
 - Schematy połączeń
 - Adresacja IP
 - Dostęp do wdrażanych urządzeń i systemów umożliwiających swobodną zmianę konfiguracji czy wykonywania aktualizacji bez udziału Wykonawcy, Producenta czy innych osób trzecich.
 - Pliki z konfiguracją wdrażanych urządzeń
 - Dokumentacja Powykonawcza musi zostać dostarczona na szyfrowanym nośniku. Nośnik musi spełniać wymagania NATO pod kątem skuteczności ochrony danych (szyfrowanie)

Zadanie 40. Testy bezpieczeństwa infrastruktury sieciowej OT/ICS/IloT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usługi przeprowadzenia testów bezpieczeństwa infrastruktury sieciowej w środowiskach OT, ICS oraz IloT, mających na celu ocenę poziomu bezpieczeństwa, identyfikację podatności oraz weryfikację odporności infrastruktury na zagrożenia cybernetyczne, zgodnie z wymaganiami Zamawiającego.

2. Wymagania dotyczące usługi

2.1. Zakres testów bezpieczeństwa

- Wykonawca zobowiązany jest do przeprowadzenia testów bezpieczeństwa infrastruktury sieciowej środowisk OT/ICS/IIoT Zamawiającego obejmujących analizę architektury sieci, konfiguracji urządzeń, komunikacji pomiędzy zasobami oraz mechanizmów ochrony wdrożonych w infrastrukturze przemysłowej.
- Testy bezpieczeństwa muszą być prowadzone w sposób nienaruszający ciągłości pracy systemów technologicznych oraz bez ingerencji w proces technologiczny.

2.2. Metodyka realizacji testów

- Testy bezpieczeństwa muszą być realizowane wyłącznie w oparciu o:
 - analizę architektury sieci przemysłowej,
 - analizę komunikacji pomiędzy zasobami infrastruktury OT,
 - analizę konfiguracji urządzeń infrastruktury sieciowej,
 - analizę zdarzeń bezpieczeństwa generowanych przez systemy ochrony infrastruktury OT,
 - analizę anomalii komunikacyjnych w ruchu sieciowym.
- Testy muszą być realizowane w sposób pasywny, bez generowania dodatkowego ruchu w sieci przemysłowej, z wykorzystaniem jedynie wdrożonych systemów cyberbezpieczeństwa OT

2.3. Zakaz stosowania narzędzi skanujących

- W trakcie realizacji testów bezpieczeństwa zabrania się stosowania narzędzi automatycznego skanowania infrastruktury sieciowej.
- W szczególności niedopuszczalne jest stosowanie:
 - skanerów podatności,
 - skanerów portów,
 - narzędzi automatycznego wykrywania usług sieciowych,
 - narzędzi aktywnego fingerprintingu urządzeń,
 - narzędzi generujących ruch testowy w sieci OT.
- Testy bezpieczeństwa nie mogą polegać na aktywnym skanowaniu infrastruktury przemysłowej ani generowaniu ruchu mogącego zakłócić komunikację pomiędzy urządzeniami przemysłowymi.

2.4. Wykorzystanie wdrożonych systemów bezpieczeństwa OT

- Testy bezpieczeństwa muszą być realizowane z wykorzystaniem wdrożonych w infrastrukturze Zamawiającego systemów bezpieczeństwa przeznaczonych dla środowisk OT.
- W szczególności wykonawca zobowiązany jest do wykorzystania danych oraz mechanizmów detekcji dostępnych w systemach:
 - monitorowania komunikacji przemysłowej,
 - detekcji anomalii w komunikacji sieciowej,
 - analizy zdarzeń bezpieczeństwa infrastruktury OT.
- Analiza musi obejmować w szczególności:
 - korelację zdarzeń bezpieczeństwa,
 - analizę komunikacji pomiędzy zasobami infrastruktury,
 - analizę relacji komunikacyjnych pomiędzy strefami bezpieczeństwa.

2.5. Analiza architektury sieci

- W ramach testów bezpieczeństwa wykonawca zobowiązany jest do przeprowadzenia analizy architektury infrastruktury sieciowej OT obejmującej w szczególności:
 - identyfikację stref bezpieczeństwa infrastruktury przemysłowej,
 - analizę segmentacji sieci,
 - analizę komunikacji pomiędzy strefami infrastruktury,
 - analizę połączeń pomiędzy siecią OT, siecią IT oraz systemami zewnętrznymi.

2.6. Analiza konfiguracji urządzeń infrastruktury

- Testy bezpieczeństwa muszą obejmować analizę konfiguracji urządzeń infrastruktury sieciowej OT, w szczególności:
 - konfiguracji mechanizmów filtracji ruchu,
 - konfiguracji reguł firewall,
 - konfiguracji mechanizmów kontroli dostępu,
 - konfiguracji mechanizmów segmentacji sieci.

2.7. Ochrona procesu technologicznego

- W trakcie realizacji testów bezpieczeństwa wykonawca zobowiązany jest zapewnić, że prowadzone działania nie spowodują:
 - zakłócenia komunikacji pomiędzy urządzeniami przemysłowymi,
 - ingerencji w pracę systemów sterowania,
 - wpływu na ciągłość pracy procesów technologicznych.
- Testy bezpieczeństwa muszą być prowadzone w sposób nienaruszający deterministycznego charakteru komunikacji przemysłowej.

2.8. Raport z testów

- Wyniki przeprowadzonych testów bezpieczeństwa muszą zostać przedstawione w formie raportu zawierającego co najmniej:
 - opis architektury infrastruktury sieciowej,
 - identyfikację zidentyfikowanych podatności i ryzyk,
 - ocenę poziomu ryzyka dla poszczególnych zasobów infrastruktury,
 - rekomendacje działań korygujących,
 - priorytety realizacji działań naprawczych.

2.9. Osoby wykonujące testy

- Wymagane jest aby osoby przeprowadzające testy legitymowały się certyfikatami wydanymi przez producenta wdrożonego systemu cyberbezpieczeństwa OT – SIEM/IDS i wdrożonych urządzeń bezpieczeństwa OT.
- Certyfikaty muszą być równoważne z poziomami CCNP lub CCIE, CCNP Security, CCNA Industrial, Ethical Hacking
- Osoby przeprowadzające testy muszą posiadać aktualny certyfikat na poziomie Industrial Cybersecurity Expert, który w zakresie egzaminów obejmował minimum
- Tematyka egzaminów certyfikacyjnych
 - ICS
 - Procesy
 - Role

- Model Purdue.
 - Omówienie warstw modelu
 - Charakterystyka komponentów warstw modelu
 - Strefy bezpieczeństwa
 - Zasady komunikacji
 - Architektura komponentów
 - Architektura sieci
- Obiekty w Purdue model:
 - Kontrolery
 - Urządzenia polowe
 - Serowniki
 - HMI
 - Historian
 - Serwery alarmowe
 - Aplikacje specjalistyczne
 - Serwery główne i nadrzędne
 - Nastawnie
 - Zakłady przemysłowe
 - SCADA
- Strefy zdemilitaryzowane i punkty styku
- Projektowanie architektury systemów zgodnych z modelem Purdue.
- Ocena zgodności systemów oraz komponentów ze standardem IEC 62443
- Definiowanie stref bezpieczeństwa oraz kanałów komunikacyjnych.
 - Charakterystyka stref bezpieczeństwa
 - Definicja kanałów komunikacyjnych
 - Punkty styku
 - Komunikacja wewnętrzna
 - Komunikacja pomiędzy strefami bezpieczeństwa
 - Komunikacja zewnętrzna
 - Wymiana danych z systemami nadrzędnymi
- Dobór i projektowanie rozwiązań ochrony stref bezpieczeństwa.
 - Agresorzy
 - Pobudki działania agresorów
 - Wektory ataku
 - Powierzchnie ataku
 - Podatności
 - Modele ataku
 - Modele wykorzystania luk bezpieczeństwa
 - Dostęp zdalny
- Zagrożenia bezpieczeństwa oraz powierzchnie ataków poszczególnych warstw modelu Purdue.
 - Symulacja ataków

- Symulacja procesów i procedur obsługi incydentów.
- Projektowanie struktur komunikacyjnych.
 - Technologia Ethernet
 - Model ISO/OSI
 - Model TCP/IP
 - Profinet
 - Modbus
 - Step7
 - Protokoły ICS w komunikacji przez sieci Ethernet w oparciu o model TCP/IP
 - Protokoły utrzymania
 - Protokoły kontrolne
 - Protokoły aplikacyjne
 - Szyfrowanie danych
 - Szyfrowanie transmisji
 - Tunelowanie protokołów
 - Technologie bezprzewodowe w przemyśle
- Projektowanie systemów przemysłowych.
 - ICS
 - DCS
 - SCADA
 - PI
 - Historian
 - HMI
 - PLC
 - PCM
 - PCS
- Architektura struktur serwerowych
 - Systemy operacyjne Windows
 - Systemy operacyjne Linux
 - Systemy operacyjne UNIX
- Architektura systemów bezpieczeństwa sieci przemysłowych.
 - Firewall
 - ZBWF
 - IDS
 - IPS
 - Diody danych
 - Sondy
 - Kopia ruchu
 - Analiza ruchu
 - Kontrola dostępu
 - Monitoring
 - SIEM

- SOAR
- Architektura systemów utrzymania sieci oraz systemów przemysłowych
 - Kontrola dostępu
 - Systemy kopii zapasowych
 - Systemy odtwarzania
 - Monitoring
- Rozwiązania bezpieczeństwa w infrastrukturze przemysłowej.
 - Kryptografia w przemyśle
 - Typy ataków
 - Atak kierowany na rozwiązania przemysłowe
 - Zakłócenia obiektowe
 - Bezpieczne wykonywanie kopii zapasowych
 - Bezpieczne skanowanie podatności
 - Bezpieczna aktualizacja systemu
- Projektowanie rozwiązań IT do bezpiecznego wdrożenia w infrastrukturze przemysłowej.

Zadanie 41. Usługi konfiguracji i hardeningu systemów/urządzeń OT

1. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa profesjonalnej konfiguracji bezpieczeństwa (Hardening) oraz optymalizacji systemów przemysłowych (OT). Celem jest zminimalizowanie powierzchni ataku (Attack Surface) oraz uszczelnienie komunikacji między siecią korporacyjną a infrastrukturą przemysłową

2. Wymagania dotyczące zakresu prac:

2.1. Hardening Systemowy (System-Level Hardening)

- Redukcja usług: Wyłączenie zbędnych protokołów, portów oraz usług systemowych niekrytycznych dla procesu technologicznego na serwerach.
- Zarządzanie dostępem: Konfiguracja rygorystycznych zasad haseł.

2.2. Bezpieczeństwo Sieciowe i Separacja (Network Hardening)

- Segmentacja OT: Fizyczna lub logiczna (Virtual Bridge, VLAN, ACL) separacja sieci produkcyjnej od sieci biurowej zgodnie z normą IEC 62443.

2.3. Odporność Urządzeń (Device Hardening)

- Logowanie zdarzeń: Konfiguracja i optymalizacja systemów bezpieczeństwa ich zbierania logów w celu wykrywania włamań.

Postanowienia końcowe i wymagania wobec dostaw i Wykonawcy dla części 2

- Wykonawca lub podmiot, na którego zasobach Wykonawca polega przy realizacji zamówienia, musi posiadać aktualny certyfikat zgodności z normą ISO/IEC 27001 oraz musi zapewnić wsparcie techniczne w języku polskim, świadczone w dni robocze od poniedziałku do piątku w godzinach 08:00-16:00.
- Szkolenia: Szkolenie dla administratorów Zamawiającego w zakresie konfiguracji i bieżącej obsługi oferowanego rozwiązania przeprowadzone zostaną w języku polskim. Szkolenie musi być przeprowadzone bezpośrednio przez producenta lub autoryzowanego dystrybutora rozwiązania. Zakończone potwierdzającym umiejętności certyfikatem.

Rozwiązania równoważne i wieloproducentowe (Multivendor)

1. Zamawiający dopuszcza budowę systemu w oparciu o rozwiązania różnych producentów, pod warunkiem spełnienia minimalnych funkcjonalności OPZ i zachowania pełnej spójności technologicznej, interoperacyjności oraz spełnienia wszystkich funkcjonalności opisanych w specyfikacji.
2. W przypadku zaoferowania rozwiązań równoważnych lub pochodzących od różnych producentów, Wykonawca musi zapewnić dla nich jednolity, centralny punkt wsparcia technicznego (SPOC).