

OPIS PRZEDMIOTU ZAMÓWIENIA

(OPZ)

Dostawa, wdrożenie, asysta techniczna i szkolenie

Część nr 2 zamówienia – Zadania nr 9 i 13 wniosku o dofinansowanie (Obszar techniczny IT)

1. Przedmiot zamówienia

1.1. Zakres ogólny

Przedmiotem zamówienia jest:

1. Dostawa i wdrożenie systemu klasy SIEM/XDR opartego o platformę Wazuh w najnowszej stabilnej wersji z linii 4.14.x lub nowszej (o ile nie będzie dostępna wersja LTS wyższa) w architekturze klastrowej.
2. Konfiguracja systemu obejmująca co najmniej: kolektory logów, menedżery, indexery, dashboardy, ruleset detekcyjny zmapowany na MITRE ATT&CK, polityki retencji, RBAC oraz integrację z istniejącą infrastrukturą Zamawiającego.
3. Integracja z co najmniej minimalnym katalogiem źródeł logów.
4. Implementacja obowiązkowej biblioteki przypadków użycia (use cases) detekcyjnych.
5. Wdrożenie automatyzacji reakcji na incydenty (SOAR).
6. Integracja z źródłami Threat Intelligence
7. Opracowanie kompletnej dokumentacji powdrożeniowej.
8. Świadczenie asysty technicznej i gwarancji.
9. Przeprowadzenie szkoleń dla zespołu Zamawiającego.
10. Przekazanie wiedzy oraz wsparcie wdrożenia procedur obsługi incydentów zgodnych z NIS2/KSC. System obejmie monitorowaniem w szczególności infrastrukturę teleinformatyczną i przemysłową wykorzystywaną przy zbiorowym zaopatrzeniu w wodę, w tym środowisko OT/SCADA Stacji Uzdatniania Wody w Sanoku.

1.2. Rodzaj zamówienia i warunki licencyjne

Wskazanie platformy Wazuh jest uzasadnione, w rozumieniu art. 99 ust. 4 ustawy Pzp, obiektywnymi potrzebami Zamawiającego: wymagane jest rozwiązanie o otwartym kodzie źródłowym, pozbawione opłat licencyjnych zależnych od liczby monitorowanych zasobów, co warunkuje trwałość rezultatów projektu finansowanego ze środków KPO po zakończeniu okresu finansowania, eliminuje uzależnienie od pojedynczego dostawcy komercyjnego (vendor lock-in) oraz umożliwia samodzielne utrzymanie i rozwój reguł detekcyjnych przez Zamawiającego.

Zamawiający dopuszcza rozwiązanie równoważne, tj. platformę klasy SIEM/XDR o otwartym kodzie źródłowym, bez opłat licencyjnych za użytkowanie i bez limitów liczby monitorowanych endpointów, zapewniającą co najmniej: HIDS z kontrolą integralności plików (FIM) i oceną zgodności konfiguracji (SCA), mapowanie detekcji na MITRE ATT&CK, architekturę klastrową wysokiej dostępności, RBAC, API oraz integracje wymagane niniejszym OPZ. Ciężar wykazania równoważności spoczywa na Wykonawcy.

Zamawiający wymaga, aby dostarczona platforma Wazuh była oprogramowaniem open source na licencji GNU GPL v2 (zgodnie z oficjalnymi warunkami publikacji projektu) i aby Wykonawca nie narzucał żadnych dodatkowych ograniczeń licencyjnych. Szczegółowe warunki licencyjne:

1. Platforma Wazuh jest oprogramowaniem open source na licencji zgodnej z jego oficjalnym publikowaniem - Wykonawca potwierdzi brak opłat licencyjnych dla Zamawiającego z tytułu użytkowania platformy.
2. Licencjobiorcą wszelkich licencji komercyjnych na komponenty uzupełniające (jeśli wystąpią) będzie Zamawiający, z prawem przeniesienia na jednostki zależne.
3. Wszystkie licencje na komponenty komercyjne muszą być na czas nieoznaczony (bezterminowy).
4. Licencje nie mogą ograniczać: rozbudowy infrastruktury, liczby serwerów, rozdzielenia funkcji serwera, przeniesienia na inny serwer, tworzenia kopii zapasowych, uruchomienia na serwerach zapasowych (DR), wykorzystania na dowolnej liczbie endpointów i serwerów monitorowanych.
5. Licencja nie może być przypisana do konkretnego urządzenia ani ograniczać sposobu pracy użytkowników (praca w LAN, praca zdalna).
6. Wszelkie dedykowane rozwinięcia, reguły, dashboardy i playbooki wykonane przez Wykonawcę w ramach wdrożenia stanowią własność Zamawiającego z pełnym kodem źródłowym i dokumentacją.

2. Architektura, skala i infrastruktura

2.1. Architektura wdrożenia

~~Wykonawca zaprojektuje i wdroży architekturę uwzględniającą wysoką dostępność oraz wymagania ciągłości działania wynikające z NIS2. Architektura musi spełniać:~~

- ~~• Klaster co najmniej 2 węzłów Wazuh Manager w trybie multi-master (primary/worker) zapewniający ciągłość działania przy awarii pojedynczego węzła.~~
- ~~• Klaster Wazuh Indexer (OpenSearch) co najmniej 3 węzły (kworum węzłów master-eligible, ochrona przed zjawiskiem split-brain) z replikacją danych (replica count $\geq$ 1), z podziałem na role master/data/ingest.~~
- ~~• Co najmniej 2 węzły Wazuh Dashboard za load balancerem z terminacją TLS.~~
- ~~• Rozdzielenie środowiska na sieci zarządzania (Management VLAN), sieci zbierania logów (Data VLAN) i sieci dostępu użytkowników (User VLAN).~~

- ~~Zapewnienie mechanizmu backupu konfiguracji, reguł i indeksów (snapshoty) do niezależnej lokalizacji geograficznej – RPO ≤ 24h, RTO ≤ 8h.~~
- ~~Obsługa środowiska Disaster Recovery~~

Wykonawca zaprojektuje i wdroży architekturę adekwatną do skali i profilu obciążenia określonych w sekcji 2.2 oraz zapewniającą wymagania ciągłości działania wynikające z NIS2.

Zamawiający dopuszcza realizację systemu w architekturze jednoserwerowej typu all-in-one, tj. z komponentami Wazuh Manager, Wazuh Indexer (OpenSearch) oraz Wazuh Dashboard uruchomionymi na jednym serwerze fizycznym (dopuszczalny podział na maszyny wirtualne w obrębie tego serwera), pod warunkiem spełnienia wszystkich wymagań funkcjonalnych, wydajnościowych i retencyjnych niniejszego OPZ. Architektura all-in-one stanowi minimalny, dopuszczalny wariant wdrożenia produkcyjnego.

Wysoka dostępność (HA) stanowi docelowy kierunek rozbudowy systemu i nie jest wymagana na etapie wdrożenia. Zamawiający wymaga jednak, aby dostarczona architektura była zaprojektowana jako skalowalna do trybu HA bez konieczności wymiany kluczowych komponentów ani ponownego wdrożenia od podstaw, tj. poprzez możliwość dołączenia kolejnych węzłów do klastra. Docelowy model wysokiej dostępności obejmuje:

- Wazuh Manager w modelu klastra master-worker: jeden węzeł master jako źródło konfiguracji, reguł i rejestracji agentów oraz co najmniej jeden węzeł worker przejmujący obsługę agentów i analizę zdarzeń, z rozkładem połączeń agentów przez load balancer.
- Wazuh Indexer (OpenSearch) w klastrze co najmniej 3 węzłów master-eligible (kworum, ochrona przed zjawiskiem split-brain) z replikacją danych (replica count >= 1) i podziałem na role master/data/ingest.
- Co najmniej 2 węzły Wazuh Dashboard za load balancerem z terminacją TLS.

Klaster Wazuh Manager działa w modelu master-worker; nie jest to architektura „multi-master”. Rolę master pełni w danym momencie dokładnie jeden węzeł, przy czym w razie awarii węzła master jego rola może zostać przejęta przez węzeł worker.

Niezależnie od wybranego wariantu (all-in-one albo HA) architektura musi spełniać:

- Rozdzielenie środowiska na sieci zarządzania (Management VLAN), sieci zbierania logów (Data VLAN) i sieci dostępu użytkowników (User VLAN).
- Mechanizm backupu konfiguracji, reguł i indeksów (snapshoty) do niezależnej lokalizacji (np. wydzielony zasób NAS): RPO ≤ 24h, RTO ≤ 8h.
- Obsługę scenariusza odtwarzania po awarii (Disaster Recovery).

W wariantcie all-in-one ciągłość działania zapewnia odtworzenie systemu z kopii zapasowej (snapshotów) w reżimie RTO ≤ 8h; wariant ten nie zapewnia automatycznego przełączenia awaryjnego (failover), które osiągalne jest dopiero w docelowym modelu wysokiej dostępności.

2.2. Skala wdrożenia

Wdrożenie ma objąć infrastrukturę Zamawiającego o następujących parametrach:

Parametr	Wartość
Liczba stacji roboczych (Windows/Linux/macOS)	170

Liczba serwerów on-premises (fizycznych i wirtualnych)	30
Liczba urządzeń sieciowych zarządzalnych (firewalle, switch'e, routery, WAF)	40
Liczba urządzeń sieci OT/ICS (jeśli występują - sterowniki, HMI, SCADA)	20
Wymagana retencja hot (indeks online, pełne wyszukiwanie)	minimum 90 dni
Wymagana retencja warm (indeks wyszukiwalny, odczyt)	minimum 365 dni
Wymagana retencja cold/archive (archiwum na potrzeby dowodowe)	minimum 24 miesiące

Na potrzeby wymiarowania infrastruktury Zamawiający przyjmuje projektowy wolumen zdarzeń: średnio 1 500 EPS oraz szczytowo 5 000 EPS. Wartości te stanowią minimalny punkt odniesienia dla doboru zasobów; Wykonawca zweryfikuje je w ramach analizy przedwdrożeniowej, a dostarczona infrastruktura musi obsłużyć wolumen nie mniejszy niż wskazany.

2.3. Dostawa infrastruktury sprzętowej

Wykonawca w ramach przedmiotu zamówienia dostarczy kompletną infrastrukturę sprzętową (lub w modelu uzgodnionym z Zamawiającym - wirtualną z zapewnieniem odpowiednich zasobów) niezbędną do uruchomienia systemu SIEM zgodnie z wymaganiami niniejszego OPZ. Zamawiający celowo nie narzuca konkretnych parametrów technicznych (liczby rdzeni, pojemności pamięci RAM, przestrzeni dyskowej, IOPS, przepustowości sieci), pozostawiając Wykonawcy - jako ekspertowi w dziedzinie - swobodę doboru platformy sprzętowej adekwatnej do zaprojektowanej architektury oraz profilu obciążenia.

Wykonawca ponosi pełną odpowiedzialność za prawidłowy dobór infrastruktury i jej zdolność do realizacji wszystkich wymagań funkcjonalnych i нефункциональных określonych w niniejszym OPZ, w tym w szczególności:

- zakładanego wolumenu zdarzeń (EPS średnie i szczytowe),
- okresów retencji hot / warm / cold zdefiniowanych w sekcji 2.2,
- wymagań wysokiej dostępności określonych w sekcji 2.1,
- parametrów wydajnościowych dashboardów i wyszukiwania retrospektywnego,
- czasu odpowiedzi systemu w warunkach obciążenia szczytowego.

Wymóg zapasu mocy.

Dostarczona infrastruktura musi posiadać zapas mocy obliczeniowej i zasobów na poziomie co najmniej 20% ponad wartość wynikającą z analizy potrzeb na dzień uruchomienia produkcyjnego (Go-Live). Zapas ten dotyczy wszystkich kluczowych wymiarów zasobów: mocy obliczeniowej (CPU), pamięci operacyjnej (RAM), przestrzeni dyskowej, wydajności operacji wejścia-wyjścia (IOPS) oraz przepustowości interfejsów sieciowych. Celem tego zapasu jest zapewnienie bezpiecznego buforu na:

- wzrost wolumenu logów wraz z rozbudową monitorowanej infrastruktury,

- szczyty obciążenia podczas trwających incydentów bezpieczeństwa (kiedy liczba zdarzeń gwałtownie rośnie),
- dodawanie nowych use case'ów detekcyjnych zwiększających obciążenie silnika korelacji,
- realizację wyszukiwań retrospektywnych i zapytań ad-hoc bez wpływu na bieżący ingest.

Uzasadnienie doboru

Wykonawca w ofercie oraz w dokumencie Low-Level Design (LLD) przedstawi uzasadnienie doboru infrastruktury wraz z kalkulacją, z której wynika zachowanie wymaganego 20-procentowego zapasu. Uzasadnienie musi obejmować metodologię szacowania oraz przyjęte założenia (m.in. średni rozmiar zdarzenia, współczynnik kompresji, profil zapytań, liczbę równoczesnych użytkowników dashboardu).

Możliwość dalszej rozbudowy.

Niezależnie od powyższego, Zamawiający wymaga, aby dostarczona infrastruktura zapewniała możliwość dalszej rozbudowy w horyzoncie co najmniej 3 lat bez konieczności wymiany kluczowych komponentów - np. poprzez niewykorzystane sloty pamięci, możliwość dołożenia dysków, wolne porty sieciowe lub możliwość dołączenia kolejnych węzłów do klastra.

Skutki niespełnienia wymagań.

W przypadku stwierdzenia - w trakcie eksploatacji lub testów akceptacyjnych - że dostarczona infrastruktura nie spełnia wymagań wydajnościowych lub nie zapewnia deklarowanego zapasu mocy, Wykonawca na własny koszt dokona jej rozbudowy lub wymiany do stanu zgodnego z OPZ, bez wpływu na harmonogram projektu i bez dodatkowych roszczeń wobec Zamawiającego.

2.4. Bezpieczeństwo samego systemu SIEM (secure-by-design)

1. Platforma Wazuh zostanie utwardzona zgodnie z CIS Benchmarks dla jej komponentów oraz systemu operacyjnego, z udokumentowanymi odstępstwami.
2. Multi-Factor Authentication (TOTP lub FIDO2) wymagane dla każdego konta administracyjnego i analityka - integracja z IdP Zamawiającego (Entra ID / AD).
3. Rozdzielenie obowiązków (Separation of Duties) - konta administratorów systemu, operatorów SOC, audytorów i osób tworzących reguły mają rozdzielne uprawnienia RBAC.
4. Konta lokalne tylko w trybie break-glass, przechowywane w sejfie haseł, z automatyczną rotacją i alertem przy użyciu.
5. Cała komunikacja agent-manager z wzajemną autentykacją kryptograficzną (enrollment z wykorzystaniem preshared key lub certyfikatów).
6. Izolacja sieciowa: manager nie może być dostępny z sieci użytkowników końcowych bezpośrednio.
7. Sam system SIEM monitoruje się poprzez Self-Monitoring - alarmy przy próbach modyfikacji reguł, dostępie do indeksów, wyłączaniu agentów.
8. Niezaprzeczalność logów: logi archiwalne przechowywane na magazynie z WORM (Write-Once-Read-Many) lub z kryptograficznym łańcuchem haszy (hash chain) zapewniającym wykrywalność manipulacji.

3. WYMAGANIA FUNKCJONALNE SYSTEMU

3.1. Wymagania podstawowe

System SIEM musi realizować wszystkie niżej wymienione funkcje. Zamawiający w toku testów akceptacyjnych zweryfikuje działanie każdej z nich.

1. Monitorowanie w czasie rzeczywistym aktywności sieciowej i na urządzeniach końcowych, z opóźnieniem wykrycia zdarzenia od jego wystąpienia ≤ 60 sekund dla źródeł krytycznych.
2. Centralne zbieranie, normalizacja, wzbogacanie i indeksowanie logów z wielu źródeł (syslog, Windows Event Log, pliki płaskie, API REST, Kafka, Filebeat, NetFlow/IPFIX).
3. Korelacja wielosygnałowa - tworzenie alertów na podstawie zdarzeń pochodzących z różnych źródeł w zdefiniowanym oknie czasowym.
4. Host-based Intrusion Detection (HIDS) z detekcją rootkitów, malware, nieautoryzowanych zmian.
5. File Integrity Monitoring (FIM) na krytycznych ścieżkach systemowych i aplikacyjnych, z powiadomieniami w czasie rzeczywistym.
6. Security Configuration Assessment (SCA) - regularna ocena konfiguracji systemów względem CIS Benchmarks, DISA STIG lub analogicznych benchmarków wybranych przez Zamawiającego.
7. Vulnerability Detection - skanowanie oprogramowania zainstalowanego na endpointach i korelacja z bazami CVE (NVD, feedy dostawców OS), z priorytetyzacją według CVSS i EPSS.
8. Wykrywanie malware, ransomware i zachowań anomalnych poprzez FIM, rootcheck, analizę behawioralną oraz korelację z sygnaturami.
9. Mapowanie wszystkich alertów na taktyki i techniki MITRE ATT&CK (Enterprise, Cloud, a jeśli dotyczy - ICS).
10. Analiza logów z urządzeń bez możliwości instalacji agenta (agentless) - syslog, SNMP trap, API.
11. Wsparcie co najmniej dla protokołów: Syslog (RFC 5424, 3164), Syslog-TLS, HTTPS/REST, Kafka, NetFlow v9, IPFIX, sFlow, Windows Event Forwarding.
12. Reakcja na incydenty (Active Response) - uruchamianie predefiniowanych akcji: blokada IP na firewallu, izolacja hosta, zabijanie procesu, wyłączenie konta.
13. Zaawansowane raportowanie - predefiniowane raporty zgodności (NIS2, RODO, ISO 27001, NIST 800-53, CIS Controls, PCI DSS) plus budowa raportów ad-hoc.
14. Dashboardy rolowe (executive, SOC analyst, administrator IT, auditor) z możliwością eksportu do PDF/CSV.
15. Full-text search i analiza retrospektywna na całym okresie retencji (z zastrzeżeniem warm/cold).
16. Przechowywanie surowych logów (raw events) w archiwum przez cały okres retencji.
17. Mechanizm tagowania zdarzeń (labels) i wzbogacania (enrichment) o dane kontekstowe - właściciel systemu, krytyczność, lokalizacja.
18. Microsoft Active Directory - autentykacja administratorów, analityków i audytorów (LDAPS).
19. System poczty elektronicznej - powiadomienia alarmowe z TLS i podpisem (opcjonalnie DKIM).
20. Kanał komunikacji zespołu (MS Teams, Slack, Mattermost, Rocket.Chat) - powiadomienia real-time.
21. System zarządzania sejfem haseł / PAM

3.2. Minimalny katalog źródeł logów do integracji

Wykonawca w ramach wdrożenia obligatoryjnie skonfiguruje zbieranie i analizę logów z poniższych klas źródeł. Ostateczna lista konkretnych urządzeń/systemów zostanie uzgodniona w fazie inicjacji.

Klasa źródła	Wymagane zdarzenia / moduły
Systemy operacyjne Windows	Security Event Log, System, Application, PowerShell, Sysmon (rekomendowana konfiguracja SwiftOnSecurity/Olaf Hartong), WEF z kolektorami.
Systemy operacyjne Linux/Unix	auditd, journald, /var/log/secure, /var/log/audit, sudo, SSH, cron, logi aplikacyjne.
Active Directory / DC	DC logs (security), Kerberos, NTLM, DNS, DHCP, zmiany w AD (Group Policy, utworzenie/usunięcie/modyfikacja kont i grup).
Firewall / UTM	Logi połączeń, deny, IDS/IPS, VPN (dostęp zdalny - w tym czasy i lokalizacja).
WAF	Logi ataków HTTP/S, blokady, anomalie (OWASP Top 10).
Proxy / Secure Web Gateway	Logi dostępu użytkowników do Internetu, kategoryzacja, blokady.
DNS	Logi zapytań (w tym kanały kryptograficzne: DoT/DoH), wykrywanie DGA, tuneli DNS.
Urządzenia sieciowe (switch, router)	Logi autentykacji administracyjnej, zmiany konfiguracji, błędy, port security.
Systemy EDR/XDR	Alerty, telemetria procesowa, reakcje.
Systemy bazodanowe	Audit logs (np. PostgreSQL audit, Oracle Audit Vault, SQL Server Audit), logi logowań uprzywilejowanych.
Serwery aplikacyjne i WWW	IIS, Apache, Nginx - access logs z User-Agent, błędy, próby włamań.
Wirtualizacja / hiperwizory	VMware vCenter/ESXi, Hyper-V, Proxmox - zmiany konfiguracji, logowania admin.
Backup	Status zadań backupu, anomalie, próby usunięcia kopii (wskaźnik ransomware).
Systemy tożsamości / MFA	Logi MFA, resetów haseł, eskalacji uprawnień, PAM.
Aplikacje biznesowe	Logi autentykacji i operacji uprzywilejowanych systemów krytycznych Zamawiającego.

3.3. Wymagania dotyczące dekodowników i reguł

1. Dekodery dla wszystkich źródeł z sekcji 3.2, gotowe lub dedykowane - w wersji produkcyjnej musi istnieć poprawny parsing 100% logów.
2. Biblioteka reguł własnych musi być wersjonowana w systemie kontroli wersji (GitLab/Git) i zarządzana jako "detection-as-code".
3. Reguły posiadają: unikalne ID, opis, mapowanie MITRE ATT&CK, powiązanie z ryzykiem, autora, datę ostatniej modyfikacji, status (draft/testing/production).

4. Każda nowa reguła przed wdrożeniem produkcyjnym jest walidowana w środowisku staging.
5. ~~Przegląd i tuning rulesetu w cyklach co najmniej kwartalnych (w ramach asysty technicznej).~~Przegląd i tuning rulesetu w cyklach co najmniej kwartalnych; czynność tę Zamawiający realizuje samodzielnie, siłami własnego personelu, w oparciu o przekazaną wiedzę, dokumentację oraz mechanizm detection-as-code i środowisko staging dostarczone przez Wykonawcę (poza zakresem odpłatnej asysty technicznej).

3.4. Mapowanie na MITRE ATT&CK

System musi zapewniać:

- Natywny moduł mapowania każdego alertu na taktyki i techniki MITRE ATT&CK v15 lub nowszą.
- Dashboard pokrycia - macierz MITRE ATT&CK z wizualizacją technik, dla których istnieją aktywne reguły detekcyjne.
- Raport pokrycia detekcyjnego kwartalnie, wskazujący białe plamy (braki detekcji dla technik istotnych dla Zamawiającego).
- Drill-down od techniki do konkretnych alertów i zdarzeń źródłowych.

3.5. Minimalna biblioteka use case'ów detekcyjnych

Wykonawca w ramach wdrożenia zaimplementuje i udokumentuje minimum 40 przypadków użycia z poniższej listy. Każdy use case obejmuje: regułę detekcyjną, dashboard/widok, powiadomienie, playbook reakcji, mapowanie MITRE, test walidacyjny (atomic test).

Kategoria	Przypadki użycia
Uwierzytelnianie	Brute-force SSH/RDP/VPN/webapp; Password spraying na AD; Nieudane logowania uprzywilejowane; Logowanie poza godzinami pracy; Niemożliwa podróż (impossible travel) w Entra ID; Wykorzystanie zakazanych kont serwisowych.
Eskalacja uprawnień	Dodanie konta do Domain Admins; Modyfikacja grup privileged; Użycie sudo/runas poza wzorcem; Utworzenie lokalnego konta administratora.
Malware / Ransomware	Masowa modyfikacja plików (FIM); Anomalia zapisów na udziale sieciowym; Próba usunięcia kopii VSS (vssadmin delete shadows); Wykonanie zaszyfrowanych plików; Wykonanie znanych narzędzi ransomware; Detekcja LoLBins (rundll32, mshta, regsvr32, certutil).
Persystencja	Nowy wpis w Run/RunOnce; Utworzenie zadania w Task Scheduler; Utworzenie service Windows; Modyfikacja .bash_profile, crontab, systemd services.
Lateral Movement	Wykonanie psexec/WinRM/WMI z nietypowego hosta; SMB admin share access; Pass-the-Hash / Pass-the-Ticket (Kerberos abuse).
Komendy i kontrola (C2)	Beaconing DNS; Połączenia do znanych domen C2 (TI); Tunele przez DNS/ICMP; Nietypowy User-Agent; Połączenia do IP bez PTR.
Exfiltration	Masowe odczyty danych wrażliwych; Duży wolumen do zewnętrznego storage'u; Kompresja przed transferem; Wykorzystanie chmury osobistej (OneDrive, Dropbox).

Sieć i obwód	Skanowanie portów (z wewnątrz sieci); Exploit znanej podatności CVE; Komunikacja zablokowana przez FW w szczycie ataku; Anomalia geolokalizacji IP.
Tożsamość / AD	Kerberoasting; AS-REP Roasting; Utworzenie konta ukrytego (honeypot account trigger); Modyfikacja SIDHistory; DCSync; Changes to GPO.
Integralność (FIM)	Zmiana plików krytycznych (/etc/passwd, /etc/shadow, /etc/sudoers, konfiguracja WWW); Zmiana skryptów startowych.
Podatności	Pojawienie się nowego CVE o CVSS ≥ 9 na hostach Zamawiającego; Hosty niezałatane > 30 dni; Widoczne luki w oprogramowaniu exposed do Internetu.
Ciągłość SIEM	Agent offline > 24h; Brak logów z krytycznego źródła > 1h; Próba modyfikacji konfiguracji Wazuh; Log tampering (hash mismatch).
Compliance	Wykrycie naruszenia CIS Benchmark (kategorie krytyczne); Niezgodność z polityką haseł; Wyłączenie audytu.

3.6. SOAR - automatyzacja reakcji na incydenty

System ma wspierać podstawową automatyzację reakcji zgodnie z playbookami zdefiniowanymi wspólnie z Zamawiającym. Minimalne funkcjonalności:

1. Mechanizm Active Response natywny dla Wazuh - co najmniej: blokada adresu IP (iptables/firewalld/Windows Firewall/zew. FW), izolacja hosta (endpoint isolation poprzez EDR/FW), wyłączenie konta (AD), zabicie procesu.
2. Minimum 10 gotowych playbooków zautomatyzowanych, obejmujących najważniejsze use case'y - m.in. brute-force, podejrzane logowanie z obcej geolokalizacji, ransomware indicator, exfiltracja danych, instalacja nieautoryzowanego oprogramowania.
3. Każdy playbook ma tryb "suggest" (propozycja dla analityka) oraz "auto" (pełna automatyzacja) - Zamawiający wybiera tryb dla każdej akcji.
4. Każda akcja automatyczna jest zapisana w audit logu SOAR i podlega retencji dowodowej.
5. Mechanizm "kill switch" pozwalający administratorowi na natychmiastowe wstrzymanie wszystkich automatyzacji.

3.7. Threat Intelligence (TI)

System musi być zintegrowany z zewnętrznymi źródłami wiedzy o zagrożeniach:

1. Integracja co najmniej z 3 źródłami TI publicznymi i/lub komercyjnymi, m.in.: MISP (instancja Zamawiającego lub publiczna), CERT Polska / n6, AbuseIPDB, VirusTotal API, AlienVault OTX, Shodan.
2. Wzbogacanie alertów o kontekst TI (reputacja IP, kategoria zagrożenia, powiązane kampanie).
3. Obsługa formatów STIX 2.1/TAXII 2.1.
4. Automatyczna korelacja zdarzeń z wskaźnikami IoC (IP, domeny, URL, hasze plików).
5. Możliwość wprowadzenia własnych IoC Zamawiającego w centralnym rejestrze.

3.8. Wsparcie dla obowiązków NIS2/KSC

System wspiera obowiązki podmiotu kluczowego:

1. Detekcja incydentu w czasie umożliwiającym zgłoszenie wczesnego ostrzeżenia w ciągu 24 godzin od jego wykrycia.
2. Generowanie pakietu dowodowego (evidence package) dla każdego incydentu: chronologia zdarzeń, listy hostów dotkniętych, techniki ATT&CK, surowe logi.
3. Szablony raportów zgodne z wymaganiami CSIRT sektorowego / CSIRT NASK / CSIRT GOV
4. Raportowanie kwartalne pokrycia detekcyjnego, liczby i klasyfikacji alertów, wskaźników MTTD/MTTR.
5. Retencja dowodowa - logi krytyczne w trybie WORM lub hash-chain.
6. Dashboard zgodności - widok ekspozycji kontroli (NIS2 art. 21, ISO 27001 Annex A, NIST 800-53).

D.10. Zgodność z RODO i DPIA

1. Wykonawca wesprze Zamawiającego w przygotowaniu oceny skutków dla ochrony danych osobowych (DPIA) wdrożenia SIEM - dostarczy materiały techniczne do DPIA.
2. Domyślne okresy retencji są zaprojektowane zgodnie z zasadą minimalizacji danych (Art. 5 RODO); dłuższa retencja dopuszczalna wyłącznie dla logów dowodowych.
3. System umożliwia pseudonimizację/anonimizację pól z danymi osobowymi w raportach eksportowanych poza SOC.
4. Mechanizmy realizacji praw osób, których dane dotyczą (np. możliwość wyszukania i usunięcia danych osoby z zachowaniem wymogów dowodowych - decyzje operacyjne zgodnie z polityką Zamawiającego).
5. Pełny audyt dostępu do indeksów - kto, kiedy, jakie dane wyszukał.

4. SZCZEGÓŁOWY ZAKRES WDROŻENIA

4.1 Etap I

1. Warsztaty architektoniczne z zespołem Zamawiającego - walidacja architektury, sizing, harmonogram.
2. Inwentaryzacja systemów i źródeł logów (assessment) - Wykonawca dostarcza template inwentaryzacyjny.
3. Opracowanie Low-Level Design (LLD) architektury, Configuration Baseline, listy reguł i use case'ów.
4. Sporządzenie rejestru ryzyk projektowych i planu ich mitygacji.
5. Podpisanie planu odbiorów (test plan) i kryteriów akceptacji (acceptance criteria).
6. Instalacja systemów operacyjnych na serwerach (hardened baseline - CIS Benchmark).
7. Instalacja i konfiguracja klastra Wazuh Manager.
8. Instalacja i konfiguracja klastra Wazuh Indexer.
9. Instalacja Wazuh Dashboard za load balancerem z certyfikatami TLS (CA Zamawiającego).
10. Konfiguracja MFA dla wszystkich kont.
11. Hardening platformy zgodnie z CIS Benchmarks i rekomendacjami Wazuh.
12. Konfiguracja backupu indeksów i konfiguracji.

4.2. Etap II

1. Rozmieszczenie agentów Wazuh na stacjach i serwerach Zamawiającego
2. Konfiguracja zbierania logów z urządzeń sieciowych (syslog/syslog-TLS).
3. Integracja z firewallami, WAF, proxy, DNS.
4. Opracowanie i walidacja dekodery dla wszystkich źródeł (testy poprawności parsowania > 99%).
5. Konfiguracja niezaprzeczalności logów (WORM / hash chain).
6. Konfiguracja polityki retencji (hot/warm/cold).
7. Testy wydajnościowe ingestu (EPS) na stagingu - raport testowy.
8. Implementacja minimum 40 use case'ów z sekcji 3.5
9. Integracja z feedami Threat Intelligence.
10. Konfiguracja SCA (CIS Benchmarks) na wszystkich klasach systemów.
11. Konfiguracja Vulnerability Detection - korelacja z CVE.
12. Konfiguracja FIM na krytycznych ścieżkach.
13. Konfiguracja mapowania na MITRE ATT&CK i dashboardu pokrycia.
14. Tuning reguł - redukcja false-positive (KPI: $\leq 5\%$ alertów w wyniku testów akceptacyjnych to FP).
15. Konfiguracja Active Response.
16. Konfiguracja powiadomień e-mail (szyfrowanych).
17. Integracja informacyjna z obowiązkiem raportowania do CSIRT - szablony i procedura.

4.3. Etap III Testy akceptacyjne

Testy przeprowadza się w następujących wymiarach:

- FAT (Factory Acceptance Test) - środowisko Wykonawcy, walidacja funkcjonalności bez integracji z prod.
- SAT (Site Acceptance Test) - środowisko docelowe, walidacja integracji, wydajności, HA/DR, walidacja dashboardów, raportów, procesów.
- Wykonanie ataków Atomic Red Team i MITRE Caldera; wymagane minimum 80% detekcji dla technik objętych use case'ami.
- Testy HA - awaria pojedynczego węzła nie powoduje utraty logów ani dashboardów.
- Testy DR - odtworzenie z backupu w zdefiniowanym RTO.
- Tabletop exercise - ćwiczenie z zespołem Zamawiającego scenariusza incydentu poważnego z użyciem SIEM jako narzędzia rozpoznania.

Każdy test kończy się raportem z listy checkpointów, ewentualnych niezgodności i planu ich usunięcia. Odbiór etapu następuje po usunięciu wszystkich niezgodności krytycznych i wysokich oraz po akceptacji przez komisję odbiorczą Zamawiającego.

5. DOKUMENTACJA POWDROŻENIOWA

Wykonawca dostarczy kompletną dokumentację w języku polskim (z dopuszczeniem terminologii angielskiej tam, gdzie jest ona powszechnie stosowana).

5.1. Dokumenty architektoniczne i projektowe

- HLD (High-Level Design) - architektura logiczna i fizyczna.
- LLD (Low-Level Design) - konfiguracje, parametry, adresacja, VLAN, porty, reguły FW.
- Diagramy przepływu danych (DFD) - od źródła do indeksu i archiwum.
- Rejestr integracji - lista wszystkich źródeł logów z parametrami.
- Sizing document - uzasadnienie zasobów i margines wzrostu.

5.2. Dokumenty operacyjne

- Runbook operatora - procedury codzienne (start/stop usług, sprawdzenie zdrowia, monitoring ingestu).
- Procedury awaryjne (failover, recovery, restart klastra).
- Playbooki SOC - dla każdego use case'a jeden playbook: sygnały, wstępna triage, akcje, eskalacja.
- Procedura onboarding / offboarding nowego źródła logów.
- Procedura zarządzania regułami (detection-as-code workflow).
- Procedura backup / restore / DR.
- Procedura obsługi incydentu poważnego z wykorzystaniem SIEM z powiązaniem do obowiązku zgłoszenia do CSIRT.
- Matryca ról i uprawnień (RBAC matrix).

5.3. Dokumenty zgodnościowe

- Mapa pokrycia kontroli NIS2 (art. 21), ISO 27001 Annex A 2022, NIST 800-53 Rev.5 - które kontrole wspiera SIEM.
- Materiały wspierające DPIA (RODO) - przepływy danych, retencje, bazę prawną.
- Plan ciągłości działania (BCP) i plan odtwarzania po awarii (DRP) dla systemu SIEM.
- Oświadczenie o niewystępowaniu na liście dostawców wysokiego ryzyka (DWR) zgodnie z ustawą o KSC.

5.4. Dokumenty użytkownika

- Instrukcje dla analityka SOC (operator SIEM).
- Instrukcje dla administratora IT.
- Instrukcje dla audytora wewnętrznego.
- Materiały szkoleniowe

6. SZKOLENIA I PRZEKAZANIE WIEDZY

6.1. Zakres szkoleniowy - wymóg minimum

Wykonawca przeprowadzi szkolenie z:

1. Architektura Wazuh, komponenty, klaster.
2. Instalacja, konfiguracja, aktualizacje, backupy.
3. Zarządzanie agentami (enrollment, grouping, konfiguracja).
4. Zarządzanie regułami i dekodernami (custom rules).
5. Wydajność i troubleshooting (logi, metryki, debugging).
6. Hardening i polityki bezpieczeństwa SIEM.
7. HA, DR i odtwarzanie.
8. Praca z dashboardem - przegląd alertów, wyszukiwanie, drill-down.
9. Triage incydentu - praktyczne scenariusze.
10. MITRE ATT&CK w analizie - mapowanie, threat hunting.
11. Praca z playbookami SOAR.
12. Przygotowanie pakietu dowodowego incydentu i zgłoszenia do CSIRT.
13. Threat hunting - scenariusze praktyczne.
14. Przegląd dashboardów executive.
15. Raporty zgodności (NIS2, RODO, ISO 27001).
16. KPI bezpieczeństwa - MTTD, MTTR, coverage.
17. Obowiązki kierownictwa wynikające z NIS2/KSC w kontekście SIEM.

6.2. Forma szkoleń

- Szkolenia mogą być prowadzone stacjonarnie u Zamawiającego lub zdalnie - decyzja Zamawiającego.
- Szkolenie musi być prowadzone w języku polskim przez trenera posiadającego minimum 3 lata doświadczenia praktycznego z Wazuh.
- Wszystkie sesje są nagrywane - nagrania stanowią własność Zamawiającego.

7. ASYSTA TECHNICZNA, GWARANCJA I SLA

7.1. Zakres asysty

Wykonawca świadczy asystę techniczną przez okres 24 miesięcy od dnia podpisania protokołu odbioru końcowego. Zakres asysty obejmuje:

1. Wsparcie zdalne w rozwiązywaniu problemów eksploatacyjnych (ticketing).
2. ~~Aktualizacje platformy i jej komponentów – minimum raz w kwartale zaplanowana aktualizacja, dodatkowo hotfixy krytyczne.~~ Dostarczanie aktualizacji krytycznych i poprawek bezpieczeństwa (hotfixów) platformy oraz jej komponentów. Aktualizacje planowe (niekrytyczne) pozostają poza zakresem asysty i realizowane są samodzielnie przez Zamawiającego.
3. ~~Utrzymanie reguł, dekoderek i playbooków w aktualnym stanie wobec nowych zagrożeń.~~
4. ~~Kwartalny przegląd pokrycia MITRE ATT&CK i zalecenia rozszerzenia.~~
5. ~~Cokwartalny warsztat przeglądu (service review) z KPI, ryzykami, planem.~~
6. ~~Hotline telefoniczny / email / Hotline telefoniczny oraz kanał e-mail do rejestracji zgłoszeń (incydentów, awarii i błędów), dostępny w reżimie czasowym określonym w pkt 7.2.~~

~~Zamawiający rezygnuje z obowiązkowych, cyklicznych usług eksperckich w okresie powdrożeniowym, tj. z kwartalnego przeglądu pokrycia MITRE ATT&CK oraz cokwartalnego warsztatu przeglądu (service review). Czynności te, jako powielające kompetencje przekazane Zamawiającemu w ramach transferu wiedzy, dokumentacji powdrożeniowej i szkoleń, Zamawiający realizuje samodzielnie, siłami własnego personelu, w oparciu o dostarczone mechanizmy (natywny dashboard pokrycia MITRE ATT&CK, raporty generowane przez system, detection-as-code oraz środowisko staging). Asysta techniczna świadczona jest w modelu reaktywnym, obejmującym obsługę zgłoszeń, incydentów i awarii oraz dostarczanie aktualizacji krytycznych (hotfixów bezpieczeństwa), zgodnie z poziomami usług określonymi w punkcie 7.2.~~

7.2. Poziomy usług (SLA)

~~Asysta techniczna świadczona jest w reżimie 8x5, tj. w dni robocze (od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy) w godzinach 8:00–16:00. Zgłoszenia przyjmowane poza godzinami obsługi rejestrowane są z początkiem najbliższego dnia roboczego. Czasy określone w tabeli poniżej liczone są w godzinach i dniach roboczych. Przez „czas reakcji” rozumie się potwierdzenie przyjęcia zgłoszenia i rozpoczęcie diagnozy, a przez „czas obejścia / naprawy” – przywrócenie poprawnego działania lub udostępnienie rozwiązania zastępczego (workaround).~~

<u>Priorytet</u>	<u>Definicja</u>	<u>Czas reakcji</u>	<u>Czas obejścia / naprawy</u>
<u>Krytyczny</u>	<u>Niedostępność systemu SIEM, całkowite zatrzymanie zbierania logów z krytycznych źródeł lub utrata funkcji detekcji.</u>	<u>do 4 godzin roboczych</u>	<u>do 1 dnia roboczego</u>
<u>Wysoki</u>	<u>Poważne ograniczenie funkcjonalności (np. brak działania dashboardów, zatrzymanie ingestu z części źródeł, brak alertowania) bez pełnej niedostępności.</u>	<u>do 8 godzin roboczych</u>	<u>do 3 dni roboczych</u>

Normalny	<u>Pojedyncze błędy eksploatacyjne, pytania administracyjne i drobne usterki bez wpływu na detekcję i dostępność.</u>	<u>do 2 dni roboczych</u>	<u>do 10 dni roboczych</u>
-----------------	---	---------------------------	----------------------------

Klasyfikacji priorytetu dokonuje Zamawiający w chwili zgłoszenia. Zawieszenie biegu czasów SLA możliwe jest wyłącznie na czas oczekiwania na informacje lub działania po stronie Zamawiającego, po uprzednim powiadomieniu.

8. WARUNKI UDZIAŁU W POSTĘPOWANIU

8.1. Doświadczenie Wykonawcy

W okresie ostatnich 3 lat (36 miesięcy) przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, Wykonawca należyce wykonał:

1. Co najmniej 5 wdrożeń platformy Wazuh w środowisku produkcyjnym o skali minimum 200 monitorowanych endpointów każde.
2. Co najmniej 2 wdrożenia platformy Wazuh w podmiocie objętym obowiązkami ustawy o KSC (operator usług kluczowych, podmiot kluczowy lub podmiot ważny) lub w podmiocie sektora publicznego.
3. Co najmniej 3 usługi szkoleniowe z platformy Wazuh (łącznie minimum 10 dni szkoleniowych).

Do oferty Wykonawca załączy wykaz realizacji z podaniem: nazwy podmiotu, okresu realizacji, skali (liczba endpointów), zakresu prac oraz oświadczenie o należyтым wykonaniu. Zamawiający zastrzega prawo kontaktu weryfikacyjnego.

8.2. Certyfikaty i systemy zarządzania Wykonawcy

1. Wdrożony i certyfikowany system zarządzania bezpieczeństwem informacji zgodnie z ISO/IEC 27001 (wymagany ważny certyfikat wystawiony przez akredytowaną jednostkę).
2. Wdrożeniowcy powinni posiadać certyfikacje producenta oprogramowania.
3. Oświadczenie o zgodności z wymogami NIS2/KSC w łańcuchu dostaw, w tym oświadczenie, że Wykonawca i podwykonawcy nie zostali wpisani na listę dostawców wysokiego ryzyka (DWR) zgodnie z ustawą o KSC.
4. Polisa OC Wykonawcy w zakresie działalności z minimalną sumą gwarancyjną 1 000 000 zł na jedno i wszystkie zdarzenia.