Cyberbezpieczne Wodociągi

Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

WYMAGANIA OGÓLNE 1

1. OPROGRAMOWANIE ANTYWIRUSOWE KLASY EDR/XDR DO INTEGRACJI Z SIEM – 20 LICENCJI 2

2. OPROGRAMOWANIE DO WYKONYWANIA KOPII ZAPASOWYCH Z OCHRONĄ PRZED RANSOMWARE I DEDUPLIKACJĄ – 1 SZT. 11

3. PLATFORMA SIEM – MONITOROWANIE, BADANIE PODATNOŚCI, ANALIZA I ZARZĄDZANIE LOGAMI – LICENCJA NA MIN. 50 MONITOROWANYCH HOSTÓW (ADRESÓW IP) 15

4. OPROGRAMOWANIE NAC Z FUNKCJĄ HONEYPOT – LICENCJA WIECZYSTA NA MIN. 50 URZĄDZEŃ (ADRESÓW IP) 18

5. SYSTEM IDS DLA OT WRAZ Z SONDAMI SPRZĘTOWYMI – 1 KPL. (OPROGRAMOWANIE IDS + 5 SZT. SOND) 22

6. OPROGRAMOWANIE EDR DLA OT – 5 LICENCJI 26

Zamawiający: Przedsiębiorstwo Usług Komunalnych w Zielonkach Sp. z o.o., ul. Forteczna 3, 32-086 Węgrzce

Na potrzeby postępowania pn.: „Dostawa i wdrożenie systemów cyberbezpieczeństwa w Przedsiębiorstwie Usług Komunalnych w Zielonkach Sp. z o.o.” realizowanego w ramach projektu „Wzmocnienie systemu cyberbezpieczeństwa w PUK Zielonki Sp. z o.o.” w Konkursie Grantowym „Cyberbezpieczne Wodociągi”, Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, Krajowy Plan Odbudowy i Zwiększania Odporności, finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

Wymagania ogólne

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje

produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne". Dostarczany sprzęt musi być nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż 01.01.2026 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez „wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia. Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

Zamawiający eksploatuje zapory sieciowe oparte na oprogramowaniu OPNsense. Dostarczane rozwiązania monitorujące (platforma SIEM oraz system IDS dla OT) muszą współpracować z tymi zaporami w zakresie wskazanym w opisie poszczególnych pozycji.

Dla oprogramowania dostarczanego na licencji bezterminowej (wieczystej) wygaśnięcie okresu wsparcia technicznego producenta może skutkować wyłącznie utratą dostępu do aktualizacji i pomocy technicznej. Oprogramowanie musi zachować po tym terminie pełną funkcjonalność w zakresie objętym niniejszym OPZ, bez konieczności ponoszenia przez Zamawiającego dalszych opłat licencyjnych.

1. Oprogramowanie antywirusowe klasy EDR/XDR do integracji z SIEM – 20 licencji

Licencjonowanie

Parametr	Wymaganie minimalne
Liczba licencji	20 licencji na ochronę stacji roboczych i serwerów Zamawiającego (Windows, Linux, macOS), w ramach jednej konsoli zarządzającej.
Okres licencji i wsparcia	Licencja czasowa obejmująca okres od dnia aktywacji co najmniej do dnia 31.12.2026 r., nie krócej jednak niż minimalny okres licencji nadawany natywnie przez producenta, wraz z prawem do aktualizacji oprogramowania i baz zagrożeń oraz wsparciem technicznym producenta w tym okresie.
Konsola zarządzająca	Konsola centralnego zarządzania udostępniana przez producenta w modelu chmurowym lub instalowana lokalnie w infrastrukturze Zamawiającego, umożliwiająca wspólne zarządzanie licencjami dostarczanymi w poz. 1 i poz. 6.
Integracja z SIEM	Przekazywanie zdarzeń bezpieczeństwa i incydentów do platformy SIEM dostarczanej w poz. 3 (co najmniej w formacie syslog lub przez API), umożliwiające ich korelację z pozostałymi źródłami zdarzeń.

Wspierane systemy operacyjne (stacje robocze)

Lp.	Wymaganie
1	Wsparcie dla systemów Windows 10 i 11, wszystkie oficjalne wydania/aktualizacje funkcji od Windows 10 Threshold 2 (listopad 2015) do Windows 11 25H2 (październik 2025).

Systemy operacyjne serwera

Lp.	Wymaganie
1	Wsparcie dla systemów Windows Server od wersji 2016 do 2025, w tym warianty Core (2016, 2019, 2022).

Ochrona środowisk wirtualnych (SVE)

Lp.	Wymaganie
1	Możliwość zastosowania zewnętrznego silnika skanującego (SVE) w postaci maszyny wirtualnej
2	Wsparcie SVE dla głównych platform wirtualizacyjnych: VMware (vSphere/vCenter, ESXi, Horizon, Workstation, Player), Microsoft Hyper-V/Windows Server, Proxmox VE w obsługiwanych przez producenta wersjach i aktualizacjach.

Ochrona antywirusowa i antyspyware

Lp.	Wymaganie
1	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2	Interfejs oraz wsparcie techniczne w języku polskim.
3	Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4	Wykrywanie i usuwanie aplikacji typu adware, spyware, dialer, phishing, narzędzia hakerskie, backdoor itp.
5	Wbudowana technologia ochrony przed rootkitami.
6	Skanowanie w czasie rzeczywistym plików otwieranych, zapisywanych i wykonywanych.
7	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie.
8	Skanowanie na żądanie pojedynczych plików/katalogów z poziomu menu kontekstowego.
9	Możliwość ustawienia zadania skanowania z niskim priorytetem, zmniejszającym obciążenie systemu.
10	Możliwość skanowania dysków sieciowych i przenośnych.
11	Skanowanie plików spakowanych i skompresowanych.
12	Ochrona krytycznych kluczy rejestru przed nieautoryzowanym dostępem/modyfikacją.
13	Możliwość definiowania wykluczeń na podstawie: a) pliku b) folderu c) rozszerzenia d) procesu e) hasha pliku f) hasha certyfikatu g) nazwy zagrożenia h) wiersza poleceń i) adresu IP/maski.
14	Skanowanie poczty w czasie rzeczywistym dla protokołów IMAP, MAPI, POP3, SMTP.
15	Skanowanie ruchu HTTP na stacjach roboczych z automatycznym blokowaniem zainfekowanego ruchu i powiadomieniem użytkownika w przeglądarce.
16	Blokowanie dostępu do wybranych stron internetowych wg listy administratora oraz wg gotowych kategorii producenta.
17	Wsparcie przeglądarek: Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+, Opera 21+, Brave 1.60+ bez dodatkowej konfiguracji.
18	Skanowanie ruchu sieciowego w szyfrowanych protokołach: HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS.

Lp.	Wymaganie
19	Skanowanie ruchu HTTPS transparentnie, bez konfiguracji zewnętrznych aplikacji (przeglądarek, klientów poczty).
20	Wyświetlanie w GUI na stacji (Windows/macOS) aktualnej wersji produktu i silników skanujących.
21	Wyświetlanie w GUI daty i godziny ostatniej aktualizacji.
22	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
23	Obsługa pobierania aktualizacji przez serwer proxy.
24	Możliwość ukrycia przez administratora ikony oprogramowania w obszarze powiadomień Windows.
25	Dziennik zdarzeń na stacji (Windows/macOS) rejestrujący wykryte zagrożenia oraz aktualizacje baz i oprogramowania.
26	Możliwość łączenia stacji roboczych z serwerem administracyjnym przez Internet.
27	Wbudowana funkcja komunikacji klienta z serwerem administracyjnym bez potrzeby osobnego agenta.
28	Kontrola dostępu do urządzeń na podstawie interfejsów, do których zostały podłączone.
29	Możliwość dodania zaufanych urządzeń z konsoli (na podstawie wykrycia lub ręcznie wpisanych ID urządzenia/produktu).
30	Blokowanie wysyłania informacji przez HTTP/SMTP (adresy e-mail, PIN-y, dane kont bankowych, hasła itp.).
31	Zdalna konfiguracja przez administratora reguł blokowania wysyłanych informacji.
32	Wbudowana zapora osobista z regułami na podstawie aplikacji i ruchu sieciowego.
33	Wbudowany IDS.
34	Skanowanie lokalne lub hybrydowe z weryfikacją reputacji plików w chmurze.
35	Możliwość tworzenia list sieci zaufanych.
36	Możliwość dezaktywacji funkcji zapory sieciowej.
37	Dodatkowa ochrona przed atakami typu ransomware.
38	Możliwość opóźnienia przez użytkownika restartu wymaganego do zakończenia zadań (konfigurowalne w politykach).
39	Szyfrowana komunikacja między konsolą zarządzającą a punktami końcowymi.
40	Ochrona przed exploitami – min. 15 technik wykrywania (każda możliwa do włączenia/wyłączenia, z możliwością dodania własnych procesów), w tym: a) wymuszenie DEP (Windows) b) wymuszenie relokacji modułów ASLR (Windows).
41	Ochrona przed atakami sieciowymi obejmująca m.in. techniki: pierwszy dostęp, dostęp do poświadczeń, wykrycie, crimeware, ruch boczny.
42	Ochrona przed ransomware – wykrywanie i blokowanie ataków lokalnych i zdalnych z automatycznym tworzeniem kopii plików w momencie szyfrowania oraz ich odzyskaniem (na żądanie lub automatycznie) do pierwotnej lokalizacji. Ochrona obejmuje szeroki zakres typów plików biurowych, graficznych, CAD, baz danych, archiwów i systemowych (m.in. doc/docx, xls/xlsx, ppt/pptx, pdf, jpg, png, psd, dwg, exe, dll, zip i pokrewne, łącznie kilkadziesiąt rozszerzeń).
43	Wykrywanie podatnych sterowników zainstalowanych na stacji z systemem Windows.
44	Ochrona agenta i usług antywirusowych na Windows przed próbami manipulacji i naruszenia integralności.
45	Skanowanie nośników USB przed zalogowaniem użytkownika do systemu Windows.
46	Skanowanie oprogramowania układowego UEFI.
47	Przechwytywanie TLS handshake umożliwiające skanowanie ruchu bez konieczności deszyfracji.
48	Telemetria – przesyłanie surowych danych bezpieczeństwa ze stacji Windows/macOS/Linux do SIEM (TLS 1.2+) lub ze stacji Windows/Linux do serwera Syslog (JSON).

Lp.	Wymaganie
49	Skanowanie punktów końcowych pod kątem wskaźników naruszeń bezpieczeństwa (IOC).

Stacje robocze i serwery

Lp.	Wymaganie
1	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2	Wykrywanie i usuwanie aplikacji typu adware, spyware, dialer, phishing, narzędzia hakerskie, backdoor itp.
3	Jedna wersja instalacyjna dla stacji roboczych i serwerów plików Windows.
4	Monitor antywirusowy uruchamiany automatycznie przy starcie systemu i działający nieprzerwanie do jego zamknięcia.
5	Zabezpieczenie programu przed deinstalacją przez osobę nieuprawnioną (również z prawami administratora lokalnego/domenowego) – wymóg podania hasła przy próbie deinstalacji.
6	Aktualizacja produktu i zawartości zabezpieczeń nie rzadziej niż raz na godzinę.
7	Możliwość raportowania zdarzeń informacyjnych.
8	Możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
9	Możliwość skanowania jedynie nowych i zmienionych plików.
10	Możliwość odblokowania ustawień lokalnej konfiguracji na Windows po instalacji odpowiedniego modułu, zmiana zabezpieczona hasłem.
11	Dla systemu Linux – możliwość wskazania katalogów chronionych w czasie rzeczywistym.

Ochrona Exchange

Lp.	Wymaganie
1	Filtrowanie antymalware dla ruchu mailowego przychodzącego, wewnętrznego i wychodzącego.
2	Skanowanie na żądanie oraz według harmonogramu dla skrzynek i folderów publicznych, z możliwością wykluczeń oraz ograniczenia skanowania do maili z załącznikami lub z określonego przedziału czasu.
3	Możliwość konfigurowania różnych akcji dla plików zainfekowanych, podejrzanych i niemożliwych do przeskanowania.
4	Skanowanie w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5	Skanowanie malware wewnątrz archiwów.
6	Filtr antyspamowy z możliwością białej listy adresów e-mail i domen.
7	Odpytywanie serwerów RBL zdefiniowanych przez administratora i odfiltrowywanie spamu na podstawie reputacji serwera wysyłającego.
8	Automatyczne oznaczanie jako spam wiadomości pisanych alfabetami azjatyckimi lub cyrylicą.
9	Zapytania oparte o chmurę dla ochrony przed nowym spamem.
10	Możliwość różnych akcji na wykrytym spamie: oznaczenie tematu etykietą, usunięcie, kwarantanna, przekierowanie do wskazanej skrzynki.
11	Filtrowanie zawartości dla ruchu przychodzącego, wewnętrznego i wychodzącego na podstawie tekstu lub wyrażeń regularnych w temacie/treści maila.
12	Możliwość różnych akcji dla maili dopasowanych do reguł filtrowania treści: dodanie prefiksu do tematu, usunięcie, kwarantanna, przekierowanie do wskazanej skrzynki.

Konsola zdalnej administracji

Lp.	Wymaganie
1	Centralne zarządzanie i konfiguracja ochrony wspieranych stacji i serwerów.
2	Możliwość integracji wielu domen Active Directory.

Lp.	Wymaganie
3	Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4	Podgląd z konsoli stanu ochrony punktu końcowego (ustawienia, wersja programu i bazy wirusów, wyniki skanowania na żądanie, zainstalowane moduły, ostatnia aktualizacja, przypisana polityka).
5	Możliwość utworzenia konta z rolą: administrator firmy, administrator sieci, analityk bezpieczeństwa lub ustawienia niestandardowe.
6	Podgląd z konsoli podstawowych informacji o stacji: adres IP, system operacyjny.
7	Centralna aktualizacja punktów końcowych z serwera lokalnego lub z Internetu.
8	Wysyłanie linku instalacyjnego bezpośrednio z konsoli.
9	Uruchamianie centralnej konsoli wyłącznie z poziomu przeglądarki internetowej.
10	Ręczne i automatyczne (wg harmonogramu) generowanie raportów z eksportem do PDF i CSV, w tym zbiorczo w formie archiwum ZIP.
11	Raport wg harmonogramu z możliwością automatycznego wysłania do zdefiniowanych odbiorców.
12	Możliwość generowania raportu co godzinę.
13	Pierwsza aktywacja modułu kontroli urządzeń bez konieczności restartu stacji.
14	Możliwość dodania etykiety do stacji roboczej.
15	Dezinstalacja oprogramowania antywirusowego innych producentów w trakcie instalacji zdalnej.
16	Przechowywanie kwarantanny maksymalnie 180 dni.
17	Możliwość zdefiniowania czy i co ile godzin pliki z kwarantanny są przesyłane do producenta.
18	Automatyczne przeskanowanie kwarantanny po aktualizacji zawartości bezpieczeństwa.
19	Wsparcie techniczne mailowe i telefoniczne w j. polskim (pon.–pt., 8:00–16:00), poza tymi godzinami bezpośredni kontakt z producentem 24/7 w j. angielskim.
20	Po integracji z Active Directory – automatyczne przypisywanie polityk po zalogowaniu, w zależności od użytkownika domenowego lub grupy, do której należy.
21	Automatyczne przypisywanie polityk na podstawie reguły lokalizacji określanej wg: zakresu adresów IP, adresu bramy, adresu serwera WINS, adresu serwera DNS, sufiksu DNS połączenia DHCP, możliwości rozwiązania hosta przez punkt końcowy, typu sieci, nazwy hosta.
22	Uwierzytelnienie dwuskładnikowe zgodne ze standardem RFC6238.
23	Możliwość naprawy instalacji agenta z poziomu konsoli.
24	Reguła automatycznego usuwania z konsoli punktów końcowych, które nie łączyły się przez określoną liczbę dni – z możliwością określenia wzorca nazw maszyn i godziny usunięcia.
25	Wyświetlanie adresu MAC przy nazwie hosta.
26	Wyświetlanie informacji, czy punkt końcowy jest serwerem czy stacją roboczą.
27	Wyświetlanie informacji o systemie operacyjnym punktu końcowego (Windows/Linux/macOS).
28	Filtrowanie punktów końcowych online w ostatnich 24 godzinach, 7 lub 30 dniach.
29	Menu tworzenia paczek instalacyjnych z określeniem dostępności modułu dla: stacji Windows, serwerów Windows, Linux, macOS.
30	Osobne pakiety instalacyjne dla macOS (Intel x86 i Apple M) oraz dla Windows (Intel x86 i ARM).
31	Pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli.
32	Generowanie i zapisywanie logów na stacji roboczej z poziomu konsoli.
33	Tworzenie spersonalizowanych komunikatów dla stron zablokowanych przez administratora, wg harmonogramu.
34	Zarządzanie ochroną na serwerach Exchange – tworzenie polityk i konfiguracja zdalna.
35	Znaczniki (tagi) punktów końcowych – przypisywane ręcznie lub automatycznie, z możliwością filtrowania po kilku znacznikach jednocześnie.

Lp.	Wymaganie
36	Ochrona proaktywna oparta o uczenie maszynowe, działająca przed wykonaniem, wykrywająca: a) ukierunkowane ataki b) podejrzane pliki i ruch sieciowy c) exploity d) ransomware e) grayware.
37	Odrębne działania modułu ochrony proaktywnej dla plików i dla ruchu sieciowego.
38	Tryby pracy modułu ochrony proaktywnej, zmienne przez administratora: a) tolerancyjny b) normalny c) agresywny.
39	Zintegrowany sandbox producenta z możliwością analizy pliku: a) automatyczne przesłanie ze stacji po uznaniu za podejrzany lub ręczne z konsoli b) ręczne przesłanie archiwum zabezpieczonego hasłem c) ręczne przesłanie adresu URL d) możliwość detonacji próbek pojedynczo przy jednorazowym przesłaniu wielu plików.
40	Sandbox działający w trybie monitorowania i blokowania.
41	Sandbox oferujący działania naprawcze: dezynfekcja, kwarantanna lub tylko raportowanie.
42	Sandbox z opcją wstępnego filtrowania plików (aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku) pod kątem podejrzanego zachowania.
43	Możliwość dodania rozszerzeń do wyjątków sandboxa (pliki z tym rozszerzeniem nie będą przesyłane).
44	Minimalny rozmiar pliku automatycznie przesyłanego do sandboxa: 1 KB.
45	Maksymalny rozmiar pliku automatycznie przesyłanego do sandboxa: 50 MB.
46	System zarządzania ryzykiem zintegrowany z konsolą, oceniający podatność środowiska punktami ryzyka 0–100 (im wyżej, tym większe ryzyko), obejmujący: a) wyszukiwanie i naprawę/ignorowanie podatności konfiguracji (przeglądarka, sieć, system operacyjny, luki) z określeniem nasilenia zagrożenia w punktach procentowych oraz funkcją cofnięcia zmian b) określanie luk w zainstalowanym oprogramowaniu z numerem CVE c) śledzenie i wykrywanie ryzykownych działań użytkownika z liczbą dotkniętych użytkowników i poziomem szkodliwości d) skanowanie punktów końcowych pod kątem ryzyka wg harmonogramu lub zadania jednorazowego e) raportowanie liczby urządzeń z błędną konfiguracją/lukami oraz ich ilości i szkodliwości w procentach f) wykrywanie podatności wg standardów: CIS v8.0, CMMC 2.0 (US), Cyber Essentials v3.2 (UK), Essential Eight v2023.11 (AU), HIPAA (US), SOC 2, ISO/IEC 27001:2022, PCI DSS v4.0.1, GDPR (EU), NIS2 (EU), DORA (EU).
47	Scentralizowany podgląd wykrytych zagrożeń ze wszystkich modułów ochrony w jednym miejscu, z filtrowaniem wg daty, kategorii, typu zagrożenia, działań naprawczych i innych.
48	Możliwość wymogu zmiany hasła logowania do konsoli co 90 dni.
49	Blokowanie konta w konsoli po pięciu kolejnych nieudanych próbach logowania.
50	Funkcja logowania jednokrotnego (SSO) przy integracji z Microsoft Azure.

Lp.	Wymaganie
51	Raport podsumowujący stan środowiska za ostatnie 24h/7/30 dni, obejmujący: a) zarządzane punkty końcowe b) liczbę zajętych miejsc licencji wg typu (stacje Windows, serwery Windows, macOS, Linux, urządzenia fizyczne/maszyny wirtualne) c) pięć najczęściej blokowanych zagrożeń d) podział zagrożeń na stacje i serwery e) status incydentów bezpieczeństwa f) stan modułów punktów końcowych g) ocenę ryzyka firmy h) zablokowane strony WWW (malware, phishing, oszustwa) i) zablokowane techniki ataku sieciowego (wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware).
52	Możliwość integracji z innymi systemami przez API w zakresie: raporty, licencjonowanie, konta, pakiety, incydenty, sieć, kwarantanna, integracje, Event Push Service, polityki.
53	Możliwość dobrowolnego, natychmiastowego dostępu do darmowych programów wczesnego dostępu (early access) testujących najnowsze funkcje.
54	Konsola typu Partner umożliwiająca zarządzanie wieloma firmami z jednej konsoli, w tym: a) pobieranie przez partnera plików z kwarantanny firm podległych b) zarządzanie ochroną firm podrzędnych z jednej konsoli lub tworzenie bezpośrednich dostępów dla ich użytkowników c) odseparowanie konsoli podrzędnej od konsoli partnera nadrzędnego przez administratora.
55	Profil firmy w konsoli Partner z wyborem branży (m.in. lotnictwo, budownictwo, edukacja, służba zdrowia, handel i inne).
56	Wybór trzech poziomów obciążenia procesora dla zadań skanowania wg harmonogramu (Windows, Linux, macOS).
57	Funkcja wstrzymywania skanowania podczas pracy na baterii.
58	Zmiana motywu konsoli administracyjnej (jasny, ciemny, automatyczny wg ustawień systemowych).
59	Tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na czas: 15 min, 30 min, 1 h, 2 h, 4 h, z możliwością pełnego skanowania po ponownym uruchomieniu ochrony.
60	Centrum integracji z rozwiązaniami zewnętrznymi: VMware vCenter, Veeam Backup & Replication, Microsoft Active Directory, VMware Tanzu, Microsoft Exchange (on-premises), SecurityCoach (KnowBe4).
61	Możliwość przesłania do analizy sandbox pliku z komputera zdalnego wg podanej ścieżki (maks. 100 MB).
62	Filtrowanie wykrytych incydentów bezpieczeństwa m.in. wg: ID, ostatniej aktualizacji, statusu, osoby przydzielającej, daty utworzenia, priorytetu, oceny szkodliwości (0–100), podmiotów, zasobów, ostatniej fazy killchain, wykonanych czynności, skorelowanych incydentów, typu incydentu.
63	Możliwość wygenerowania i pobrania archiwum informacji diagnostycznych z chronionych punktów końcowych (Windows, Linux, macOS), zawierającego co najmniej: dla Windows – logi zainstalowanego agenta, dziennik zdarzeń Windows, informacje o systemie, DnsCache, Webcache, informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY), harmonogram zadań, historię PowerShell (jeśli włączona); dla Linux – podstawowy log pomocy technicznej agenta, certyfikaty, autorun i usługi, informacje sieciowe, informacje systemowe, zainstalowane pakiety.

Lp.	Wymaganie
64	Przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez zapytania wykrywające m.in.: historię powłoki, wczytywanie bibliotek DLL z podejrzanej lokalizacji, sesje logowania z jawnymi danymi uwierzytelniającymi, ARP cache, IP forwarding, listę zamontowanych nośników, konfigurację iptables, połączenia TLS z certyfikatami self-signed, rozszerzenia używane w Chrome/Firefox/Safari, źródła apt (Linux), zainstalowane pakiety DEB/RPM, pakiety Python, listę użytkowników utworzonych w ciągu ostatnich 30 dni (Linux), aplikacje zdalnego dostępu w macOS, status Kontroli Kont Użytkowników (UAC), status SecureBoot, listę zapamiętanych sieci bezprzewodowych, zmiany domyślnego folderu startowego użytkownika/maszyny.
65	Możliwość tworzenia konfigurowalnych reguł generujących incydent bezpieczeństwa po spełnieniu warunków, w tym: a) automatyczne działania po spełnieniu warunków (izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i inne), zależne od wybranej kategorii b) tworzenie reguł przez wybór operatora (np. „to”, „zawiera”, „jest jednym z”) c) reguły dotyczące określonych kryteriów (proces, plik, rejestr, połączenia) d) możliwość tworzenia zapytań YARA e) określenie priorytetu kolejności automatyzacji f) wybór przez administratora poziomu szkodliwości generowanych incydentów (wysoki, średni, niski).

EDR – Endpoint Detection and Response

Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.

Komponenty EDR

Lp.	Wymaganie
1	Sensor EDR gromadzący i przetwarzający dane o punkcie końcowym i zachowaniu aplikacji w celu raportowania.
2	Analityka Bezpieczeństwa – komponent interpretujący metadane gromadzone przez sensor EDR.
3	Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR na Windows, rozszerzającego ochronę świadczoną równolegle przez inny produkt antywirusowy.

Wykrywanie podejrzanej aktywności

Lp.	Wymaganie
1	Monitorowanie zdarzeń na punktach końcowych pod kątem oznak ataku, oparte o techniki MITRE ATT&CK i własną inteligencję zagrożeń, z wywoływaniem incydentów po wykryciu.
2	Zgłaszanie naruszeń jako incydentów w module EDR.

Badanie incydentów i wizualizacja

Lp.	Wymaganie
1	Wsparcie analizy incydentów narzędziami do filtrowania, badania i podejmowania działań wobec wszystkich zdarzeń bezpieczeństwa wykrytych przez sensor EDR w określonym czasie.
2	Integracja z bazą wiedzy MITRE ATT&CK i odpowiednie oznaczanie zdarzeń bezpieczeństwa.
3	Zaawansowana wizualizacja zdarzeń bezpieczeństwa obejmująca: a) kartę podsumowującą z przeglądem wpływu zdarzenia i szczegółami każdego węzła b) oś czasu zbierającą informacje o rozwoju zdarzenia w kolejności chronologicznej c) gromadzenie informacji o działaniach podjętych przez produkt w związku ze zdarzeniem.

Incydenty

Lp.	Wymaganie
1	Informowanie o wykrytych i zablokowanych zagrożeniach w formie grafu i chronologicznej linii zdarzeń, z możliwością: a) filtrowania zdarzeń b) zakończenia procesów c) dodania procesów do czarnej listy d) dodania procesów do białej listy e) izolacji hosta f) przesłania pliku do sandboxa g) sprawdzenia informacji o pliku w Google h) sprawdzenia informacji o pliku w VirusTotal.
2	Szybki podgląd incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
3	Blokowanie na podstawie reguł czarnej listy w kategoriach: a) hash MD5 lub SHA256 b) pełna ścieżka do aplikacji c) reguła połączenia.
4	Import reguł czarnej listy (hash, ścieżki, reguły połączeń) z pliku CSV.
5	Szeroki zakres filtrowania reguł blokowania minimum wg: nazwy pliku, hasha pliku, typu hasha, ścieżki, protokołu, portu/zakresu portów, daty dodania.
6	Możliwość wygenerowania i wyeksportowania listy incydentów do pliku CSV.

Patch Management / Zarządzanie Aktualizacjami

Lp.	Wymaganie
1	Wsparcie dla systemów Windows: Windows 11, Windows 10, Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016.
2	Wsparcie dla systemów Linux (64-bit): CentOS 7 (GA+ 7.2003), Red Hat Enterprise Linux RHEL 7 (GA+ 7.1–7.9), Red Hat Enterprise Linux RHEL 8 (GA+ 8.4), SUSE Linux Enterprise SLES 12 (GA+ SP5), SUSE Linux Enterprise SLES 15 (GA+ SP5), SUSE Linux Enterprise SLED 15 (GA+ SP5).
3	Możliwość działania w trybie automatycznym obejmująca: a) wykrycie i wylistowanie brakujących kompatybilnych łatek b) zaplanowanie oddzielnej automatycznej instalacji wg kategorii poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami) c) możliwość opóźnienia ponownego uruchomienia, jeśli wymaga tego instalacja łatki.
4	Tryb manualny – wykrywanie i instalacja łatek na żądanie.
5	Podgląd wszystkich kompatybilnych brakujących łatek ze wspieranych punktów końcowych, zebranych w zakładce inwentarza aktualizacji, w tym: a) sprawdzenie, które punkty końcowe mają zainstalowane/brakujące aktualizacje b) informacja zwrotna w razie niepowodzenia instalacji łatki c) szybka instalacja brakujących łatek na urządzeniu d) możliwość dodania przez administratora jednej lub wielu łatek do czarnej listy.
6	Raportowanie brakujących łatek z perspektywy punktu końcowego (zainstalowane/brakujące na każdym punkcie końcowym).
7	Pobieranie aktualizacji przez serwer pośredniczący (Windows) lub bezpośrednio przez Internet.
8	Skanowanie dostępnych aktualizacji dla nowo zainstalowanych kompatybilnych aplikacji na punkcie końcowym.
9	Wyświetlanie listy numerów CVE dla podatności naprawianych przez daną aktualizację.

2. Oprogramowanie do wykonywania kopii zapasowych z ochroną przed ransomware i deduplikacją – 1 szt.

Charakterystyka minimalna

Lp.	Wymaganie
A. Licencjonowanie i architektura	
A.1	Oprogramowanie dostarczone w modelu licencji bezterminowej (wieczystej / perpetual), z prawem do pobierania aktualizacji i poprawek w okresie obowiązującego wsparcia technicznego.
A.2	Licencjonowanie w modelu uniwersalnym, opartym na liczbie chronionych instancji (obciążeń) – min. 10 urządzeń, umożliwiające wymienną ochronę maszyn wirtualnych, serwerów fizycznych, stacji roboczych oraz obciążeń chmurowych w ramach tej samej puli licencji.
A.3	Brak ograniczeń licencyjnych co do liczby repozytoriów kopii zapasowych oraz ich komponentów (extentów).
A.4	Możliwość wdrożenia w postaci gotowego, prekonfigurowanego obrazu zawierającego zahartowany, minimalny system operacyjny klasy Linux wraz z oprogramowaniem backupu.
A.5	Obsługa wdrożenia także w postaci instalatora dla systemów Microsoft Windows (instalacja graficzna oraz nienadzorowana z linii poleceń).
A.6	Dostępność minimalnego, dedykowanego obrazu systemu dla komponentów infrastruktury: serwerów proxy, repozytoriów, serwerów montujących i bram.
A.7	Wbudowany mechanizm automatycznej aktualizacji komponentów (systemu operacyjnego appliance oraz aplikacji) przez interfejs webowy lub linię poleceń.
A.8	Wbudowana deduplikacja oraz kompresja danych kopii zapasowych, ograniczająca wolumen kopii przechowywanych w repozytoriach.
A.9	Wsparcie techniczne producenta, obejmujące prawo do aktualizacji i nowych wersji oprogramowania oraz zgłaszania błędów, na okres od dnia dostarczenia licencji co najmniej do dnia 31.12.2026 r., nie krócej jednak niż minimalny okres wsparcia nadawany natywnie przez producenta wraz z licencją.
B. Ochrona środowisk wirtualnych	
B.1	Backup i odtwarzanie maszyn wirtualnych VMware vSphere oraz Microsoft Hyper-V, w tym natychmiastowe odtworzenie całej maszyny oraz odtwarzanie granularne elementów aplikacji.
B.2	Backup bezagentowy (agentless) z wykorzystaniem mechanizmu śledzenia zmienionych bloków (CBT) oraz przetwarzania spójnego z aplikacją.
B.3	Natychmiastowe odtworzenie (Instant Recovery) maszyny uruchamianej bezpośrednio z pliku kopii do środowiska VMware, Hyper-V.
B.4	Backup z migawek macierzy produkcyjnych (storage snapshots) wiodących producentów, z minimalnym wpływem na środowisko produkcyjne.
B.5	Wbudowana akceleracja WAN przyspieszająca transfer kopii i replik do lokalizacji zdalnej oraz oszczędzająca pasmo.
B.6	Kontrola maksymalnego opóźnienia pamięci masowej (storage latency control), aby zadania backupu i replikacji nie wpływały na dostępność produkcji.
B.7	Przechowywanie każdej maszyny wirtualnej w osobnym pliku kopii (per-VM) z równoległym przetwarzaniem oraz powinowactwem proxy i repozytorium.
C. Ochrona serwerów i stacji roboczych (agenci)	
C.1	Backup agentowy serwerów i stacji roboczych Windows, Linux oraz macOS, z automatycznym wdrażaniem i zarządzaniem agentami z poziomu centralnej konsoli.
C.2	Agenci zoptymalizowani pod chmurę (cloud-integrated) zapisujący kopie bezpośrednio do pamięci obiektowej i działający bez bezpośredniego połączenia sieciowego.
C.3	Organizacja i automatyzacja wdrożeń agentów w oparciu o kontenery Active Directory, pliki CSV lub tagi chmurowe (grupy ochrony) z harmonogramami aktualizacji.

Lp.	Wymaganie
D. Ochrona aplikacji i baz danych	
D.1	Tworzenie kopii spójnych z aplikacją (application-aware) z obsługą backupu logów transakcyjnych dla Microsoft SQL Server.
D.2	Dedykowane wtyczki do backupu baz/aplikacji Microsoft SQL, z centralnym zarządzaniem politykami backupu.
D.3	Granularne odtwarzanie elementów aplikacji za pomocą dedykowanych narzędzi dla: Microsoft SQL Server, Microsoft Active Directory.
D.4	Natychmiastowe odtworzenie bazy danych (Microsoft SQL Server) do stanu bieżącego lub do wskazanego punktu w czasie.
D.5	Backup i odtwarzanie Microsoft Entra ID wraz z profilami konfiguracji oraz politykami zgodności urządzeń Intune.
E. Ochrona obciążeń chmurowych	
E.1	Natywny backup i odtwarzanie zasobów AWS z odtwarzaniem pełnym i granularnym do tego samego lub innego konta/regionu.
E.2	Natywny backup i odtwarzanie zasobów Microsoft Azure
E.3	Natywny backup i odtwarzanie zasobów Google Cloud
E.4	Natywne wykonywanie migawek oraz backup obrazowy i agentowy obciążeń IaaS/PaaS u wiodących dostawców chmury.
E.5	Backup pamięci obiektowej z możliwością odtworzenia do innego typu pamięci.
E.6	Mechanizmy kontroli kosztów chmury (kompresja, przenoszenie do archiwalnych klas pamięci, prognozowanie kosztów i planowanie pojemności).
E.7	Natychmiastowe odtworzenie obciążeń do Microsoft Azure
E.8	Migracja kopii i obciążeń pomiędzy chmurami oraz pomiędzy chmurą a środowiskiem lokalnym (AWS, Azure, Google Cloud, on-premises).
F. Repozytoria, magazyny kopii i szyfrowanie	
F.1	Obsługa repozytorium zahartowanego opartego na systemie Linux z niezmiennością (immutability) kopii, uniemożliwiającą ich zaszyfrowanie lub usunięcie przez ransomware i nieuprawnionych użytkowników.
F.2	Składowanie kopii w pamięci obiektowej (object storage) lokalnej oraz w chmurze publicznej z niezmiennością opartą o blokadę obiektów (S3 Object Lock).
F.3	Repozytorium typu scale-out z automatycznym zarządzaniem cyklem życia kopii w warstwach: wydajnościowej, pojemnościowej i archiwalnej.
F.4	Warstwa archiwalna z natywną obsługą Amazon S3 Glacier (w tym Glacier Deep Archive) oraz Microsoft Azure Archive Storage.
F.5	Szyfrowanie typu end-to-end algorytmem AES-256 dla danych w źródle, w trakcie transmisji oraz w spoczynku.
F.6	Przenoszenie i kopiowanie plików kopii pomiędzy zadaniami i repozytoriami oraz proaktywna weryfikacja stanu warstwy pojemnościowej (health-check).
F.7	Realizacja reguły 3-2-1 poprzez zadania kopiowania kopii (backup copy) z walidacją i naprawą; zewnętrzne repozytorium do odtwarzania z kopii chmurowych.
F.8	Backup udziałów plikowych NAS (SMB i NFS) z archiwizacją wersji plików oraz backup danych w pamięci obiektowej.
F.9	Integracja z gotowym, chmurowym magazynem obiektowym dostawcy oraz backup off-site za pośrednictwem usługodawcy.
G. Ochrona przed ransomware i bezpieczeństwo platformy	
G.1	Wbudowany silnik wykrywania złośliwego oprogramowania działający w trakcie backupu (analiza indeksu plików, wykrywanie szyfrowania i podejrzanych rozszerzeń) z oznaczaniem punktów przywracania jako podejrzane/zainfekowane/czyste.

Lp.	Wymaganie
G.2	Wbudowane, niskoobciążeniowe skanowanie sygnaturowe zagrożeń z aktualizowaną w czasie rzeczywistym bazą sygnatur.
G.3	Skanowanie zawartości kopii regułami YARA (m.in. w ramach testów odtwarzalności, bezpiecznego odtwarzania oraz skanowania na żądanie).
G.4	Skaner wskaźników kompromitacji (IoC) wykrywający narzędzia atakujących oraz narzędzia służące do eksfiltracji danych.
G.5	Analiza taktyk, technik i procedur atakujących (TTP) chroniąca serwery backupu przed cyberatakiem.
G.6	Bezpieczne odtwarzanie (Secure Restore) z opcjonalnym skanem antywirusowym/YARA pliku kopii przed przywróceniem do produkcji.
G.7	Centralne zarządzanie kluczami kryptograficznymi poprzez integrację z systemem zarządzania kluczami (KMS).
G.8	Integracja z systemami klasy SIEM/SOAR oraz ITSM (m.in. Splunk, Microsoft Sentinel, Palo Alto XSIAM/XSOAR, ServiceNow, CrowdStrike) oraz przekazywanie zdarzeń do serwerów syslog.
G.9	Otwarte API incydentów umożliwiające narzędziom cyberbezpieczeństwa oznaczanie punktów przywracania jako zainfekowane lub wyzwalanie backupu.
G.10	Autoryzacja dwuosobowa (zasada czterech oczu) dla operacji destrukcyjnych: usuwania kopii i repozytoriów, dodawania administratorów, zmian uprawnień i MFA.
G.11	Uwierzytelnianie wieloskładnikowe (MFA) konsoli oraz obsługa federacyjnego logowania jednokrotnego (SSO).
G.12	Granularna kontrola dostępu oparta na rolach oraz audyt działań użytkowników i operacji odtwarzania plików.
G.13	Komponenty kryptograficzne zgodne ze standardem FIPS.
H. Funkcje wspomagające operatora	
H.1	Agent głębokiej analizy złośliwego oprogramowania z wizualizacją zagrożeń, oceną ich wpływu oraz prowadzonymi krokami odtwarzania.
H.2	Agent analizy danych umożliwiający odpytywanie złożonych danych językiem naturalnym oraz generowanie streszczeń i rekomendacji.
H.3	Wprowadzanie głosowe usprawniające pracę operatora.
H.4	Codzienne podsumowanie odporności danych korelujące wykryte problemy z bazą wiedzy producenta oraz listą rekomendowanych działań.
H.5	Interaktywne, inteligentne raportowanie ułatwiające analizę i podejmowanie decyzji.
H.6	Asystent czatu wspierający rozwiązywanie problemów i optymalizację.
I. Odtwarzanie i replikacja	
I.1	Odtwarzanie całych maszyn wirtualnych do lokalizacji oryginalnej lub nowej oraz odtwarzanie pojedynczych dysków i plików maszyn.
I.2	Natychmiastowe odtwarzanie pojedynczych dysków, baz danych oraz udziałów plikowych bezpośrednio z pliku kopii.
I.3	Odtwarzanie plikowe z systemów Windows, Linux, macOS w tym porównanie z produkcją, odtwarzanie uprawnień oraz indeksowanie systemu plików gościa.
I.4	Ciągła ochrona danych (CDP) dla obciążeń krytycznych z odtwarzaniem do stanu bieżącego lub wybranego punktu w czasie, w tym CDP dla dowolnych maszyn Windows (fizycznych, wirtualnych i chmurowych).
I.5	Odtwarzanie plików i aplikacji z repliki CDP z dowolnego punktu przywracania, bez przerywania replikacji.
I.6	Replikacja obrazowa maszyn wirtualnych lokalnie oraz do lokalizacji zapasowej, z asystowanym przełączaniem awaryjnym i powrotem (failover/failback) oraz replikacją tworzoną z plików kopii.

Lp.	Wymaganie
I.7	Orkiestracja przełączania awaryjnego jednym kliknięciem (plany failover) oraz replikacja do chmury usługodawcy (DRaaS).
I.8	Automatyczna weryfikacja odtwarzalności replik poprzez próbny failover w odizolowanym środowisku, z obsługą własnych skryptów.
I.9	Odtwarzanie oraz migracja maszyn lokalnych bezpośrednio do chmur AWS, Microsoft Azure i Google Cloud.
I.10	Udostępnianie zawartości kopii aplikacjom i skryptom firm trzecich poprzez API integracji danych (do analiz bezpieczeństwa, kontroli zgodności i ponownego wykorzystania danych).
J. Weryfikacja odtwarzalności i środowiska testowe	
J.1	Automatyczne testowanie i weryfikacja odtwarzalności każdej kopii poprzez uruchomienie maszyny z pliku kopii w odizolowanym (fenced-off) środowisku, wraz z obsługą własnych skryptów testowych.
J.2	Piaskownica na żądanie (on-demand sandbox) umożliwiająca testowanie aktualizacji, rozwiązywanie problemów i szkolenia bez wpływu na produkcję.
J.3	Tworzenie środowisk testowych bezpośrednio z migawek macierzy (on-demand sandbox from storage snapshots) działających z pełną wydajnością I/O.
J.4	Odtwarzanie etapowe (staged restore) umożliwiające usunięcie danych wrażliwych z punktu przywracania przed przywróceniem do produkcji.
K. Orkiestracja odtwarzania po awarii (DR)	
K.1	Tworzenie i wykonywanie zautomatyzowanych planów odtwarzania po awarii (planów DR) z konfiguracją bez utraty danych (zero data loss).
K.2	Zautomatyzowane, nieinwazyjne testowanie planów DR w odizolowanej sieci, bez wpływu na środowisko produkcyjne, wraz ze szczegółowym raportowaniem.
K.3	Orkiestracja międzyplatformowa i planowana migracja obciążeń pomiędzy VMware, Microsoft Hyper-V / Azure Local oraz Microsoft Azure.
K.4	Orkiestracja odtwarzania kopii agentowych Windows i Linux do środowisk VMware lub Microsoft Azure.
K.5	Monitorowanie zgodności osiąganych parametrów RTO i RPO względem celów zdefiniowanych dla każdego planu DR.
K.6	Automatyczne generowanie dokumentacji planów DR (definicje, testy, wykonania) w wersji szczegółowej oraz w formie streszczenia dla kierownictwa.
K.7	Audyt planów odtwarzania ze śledzeniem zmian oraz cyklicznym raportem aktywności planów; zaplanowane kontrole gotowości (readiness checks).
K.8	Uwierzytelnianie wieloskładnikowe (MFA) zabezpieczające wykonanie i zatwierdzanie planów odtwarzania.
K.9	Skanowanie kopii pod kątem złośliwego oprogramowania na potrzeby planów odtwarzania i odtwarzanie wyłącznie z czystych punktów przywracania.
K.10	Odtwarzanie jednym kliknięciem w skali masowej (pojedyncza aplikacja lub cała lokalizacja) oraz odtwarzanie do chmury.
L. Monitorowanie i raportowanie	
L.1	Centralny pulpit prezentujący zagrożenia, ryzyka oraz ocenę poziomu bezpieczeństwa środowiska.
L.2	Monitoring wydajności i alarmowanie dla zadań backupu bez ograniczenia liczby monitorowanych serwerów backupu.
L.3	Konfigurowalne raportowanie z możliwością eksportu, raporty interaktywne oraz raportowanie chronionych baz danych.
L.4	Monitoring i raportowanie infrastruktury wirtualnej (VMware vSphere oraz Microsoft Hyper-V), w tym ocena infrastruktury wg najlepszych praktyk.
L.5	Monitoring i raportowanie ochrony obciążeń w chmurach publicznych (AWS, Microsoft Azure, Google Cloud).

Lp.	Wymaganie
L.6	Monitoring na poziomie aplikacji (m.in. wykrycie wyłączenia oprogramowania antywirusowego lub przekroczenia zasobów).
L.7	Planowanie pojemności z modelowaniem scenariuszy typu what-if oraz mapy cieplne (heatmaps) wykorzystania repozytoriów i serwerów proxy.
L.8	Widok biznesowy (business view) – kategoryzacja zasobów wg jednostki, działu, przeznaczenia i SLA, wspierająca kontrolę dostępu i zgodność.
L.9	Inteligentna diagnostyka znanych problemów oraz automatyczne działania naprawcze (self-healing remediation).
L.10	Konfigurowalne powiadomienia e-mail o alarmach oraz dwukierunkowa integracja zgłoszeń z ServiceNow.
L.11	Monitorowanie stanu wysokiej dostępności (HA) z opcjami naprawczymi oraz alarmami.
M. Zarządzanie	
M.1	Zarządzanie przez interfejs webowy (Web UI) z zaawansowanym filtrowaniem i wyszukiwaniem.
M.2	Wysoka dostępność (HA) komponentu zarządzającego z wbudowaną redundancją i przełączaniem awaryjnym (klaster HA na appliance).
M.3	Centralna, webowa konsola zarządzania rozproszonym wdrożeniem (pojedynczy panel) z możliwością uruchamiania/zatrzymywania zadań oraz wykonywania odtworzeń.
M.4	Automatyzacja zadań poprzez RESTful API oraz moduł PowerShell.
M.5	Centralne zarządzanie agentami oraz wtyczkami baz danych z poziomu konsoli.
M.6	Samoobsługowe portale odtwarzania (plików, maszyn wirtualnych, baz danych, skrzynek pocztowych) z delegacją uprawnień.

3. Platforma SIEM – monitorowanie, badanie podatności, analiza i zarządzanie logami – licencja na min. 50 monitorowanych hostów (adresów IP)

Wymagania ogólne

1) System stanowi rozwiązanie klasy SIEM/XDR przeznaczone do wykrywania zagrożeń bezpieczeństwa oraz reagowania na incydenty w infrastrukturze IT i OT Zamawiającego. Przedmiotem ochrony są końcówki (serwery, stacje robocze) objęte agentem systemu oraz urządzenia sieciowe i zabezpieczające niewspierające instalacji agenta, z których dane pozyskiwane są w trybie zdalnym za pośrednictwem protokołu syslog.

2) W zakresie ochrony końcówek system realizuje funkcje: zbierania i analizy logów systemowych oraz aplikacyjnych, monitorowania integralności plików obejmującego wykrywanie nieautoryzowanych zmian zawartości, uprawnień i atrybutów plików, oceny konfiguracji bezpieczeństwa systemów operacyjnych względem przyjętych standardów (m.in. CIS Benchmarks), inwentaryzacji zainstalowanego oprogramowania wraz z identyfikacją podatności na podstawie baz CVE oraz wykrywania aktywności charakterystycznej dla rootkitów i złośliwego oprogramowania.

3) Dane pozyskane z końcówek oraz z urządzeń monitorowanych bezagentowo podlegają centralnej analizie regułowej i korelacyjnej w celu identyfikacji zdarzeń wskazujących na próby nieautoryzowanego dostępu, naruszenia polityk bezpieczeństwa oraz inne symptomy incydentu, z możliwością odwzorowania wykrytych zdarzeń na taktyki i techniki opisane w macierzy MITRE ATT&CK. Wynikiem analizy są alerty bezpieczeństwa o określonym poziomie istotności, prezentowane w scentralizowanym interfejsie zarządzania wraz z kontekstem niezbędnym do oceny zasadności i podjęcia dalszych czynności.

4) System musi zapewniać funkcję automatycznej reakcji (active response) umożliwiającą wykonanie zdefiniowanej akcji zaradczej – w tym blokadę komunikacji sieciowej ze źródłem zagrożenia – bezpośrednio po wykryciu zdarzenia spełniającego określone kryteria, bez konieczności ręcznej interwencji operatora.

Wymagania szczegółowe

1. Licencja

Parametr	Wymóg minimalny
Zakres licencji	Licencja/prawo do korzystania z Oprogramowania dla min. 50 monitorowanych hostów (adresów IP)
Czas trwania	Licencja na czas nieograniczony (bezterminowa)
Limity danych	Licencja nie może ograniczać wielkości przechowywanych danych ani zakresu/czasu wyszukiwania informacji w zgromadzonych danych
Użytkownicy	Możliwość tworzenia wielu kont użytkowników oraz zapewnienia równoległego dostępu wielu użytkowników bez dodatkowych opłat licencyjnych
Wsparcie techniczne producenta/dystrybutora	Od dnia podpisania protokołu odbioru co najmniej do 31.12.2026 r., nie krócej jednak niż minimalny okres wsparcia nadawany natywnie przez producenta lub dystrybutora wraz z licencją, obejmujące możliwość zgłaszania błędów oraz aktualizację do najnowszej dostępnej wersji w okresie gwarancji
Forma dostarczenia	Licencje dostarczone do siedziby Zamawiającego w formie papierowej lub elektronicznej

2. Wymagania funkcjonalne systemu

Parametr	Wymóg minimalny
Przeznaczenie	System klasy SIEM do centralnego zbierania, analizy i korelacji logów bezpieczeństwa oraz ochrony punktów końcowych (EDR) – min. 50 monitorowanych hostów
Architektura	Architektura serwer-agent, obejmująca: moduł zarządzający (serwer), silnik indeksująco-wyszukiwawczy do przechowywania i analizy zdarzeń oraz webowy interfejs (dashboard) do wizualizacji danych
Agent punktu końcowego	Wieloplatformowy agent instalowany na końcówkach (Windows, Linux, macOS) realizujący lokalne zbieranie logów, monitorowanie integralności plików oraz ocenę konfiguracji bezpieczeństwa
Zbieranie logów z agentów	Zbieranie logów systemowych i aplikacyjnych z monitorowanych hostów i bezpieczne przekazywanie ich do serwera w celu analizy regułowej
Zbieranie logów z urządzeń bezagentowych	Odbiór i analiza logów z urządzeń niewspierających instalacji agenta (w tym urządzeń UTM/firewall) za pomocą protokołu syslog
Integracja z zaporami OPNsense	Współpraca z eksploatowanymi przez Zamawiającego zaporami OPNsense, obejmująca co najmniej: a) odbiór i analizę logów zapory, w tym logów filtra pakietów oraz modułu IDS/IPS zapory, za pośrednictwem agenta instalowanego na zaporze lub protokołu syslog, wraz z regułami umożliwiającymi wykrywanie w tych logach zdarzeń bezpieczeństwa, b) automatyczną reakcję (active response) polegającą na zablokowaniu adresu źródłowego zagrożenia na zaporze OPNsense.
Integracja z pozostałymi systemami bezpieczeństwa	Odbiór i analiza zdarzeń z oprogramowania EDR/XDR (poz. 1 i poz. 6), oprogramowania do wykonywania kopii zapasowych (poz. 2) oraz systemu IDS dla OT (poz. 5).
Analiza i korelacja zdarzeń	Analiza logów w oparciu o reguły wykrywające błędy konfiguracji, próby włamań, aktywność złośliwego oprogramowania i naruszenia polityk bezpieczeństwa, z możliwością mapowania wykrytych zdarzeń na techniki i taktyki MITRE ATT&CK
Monitorowanie integralności plików (FIM)	Wykrywanie zmian zawartości, uprawnień, właściciela i atrybutów plików na monitorowanych końcówkach

Parametr	Wymóg minimalny
Ocena konfiguracji bezpieczeństwa (SCA)	Okresowe skanowanie zgodności konfiguracji systemów operacyjnych z uznanymi standardami bezpieczeństwa (np. CIS Benchmarks) i wskazywanie wykrytych odstępstw
Wykrywanie podatności	Budowa inwentarza zainstalowanego oprogramowania na końcówkach oraz korelacja z bazami podatności (CVE) w celu identyfikacji podatnych wersji z priorytetyzacją do naprawy
Wykrywanie rootkitów	Funkcja wykrywania ukrytych procesów, plików i innych oznak aktywności typu rootkit na monitorowanych końcówkach
Aktywna reakcja (Active Response)	Możliwość automatycznego uruchomienia zdefiniowanej akcji zaradczej (np. blokady adresu źródłowego zagrożenia) w reakcji na wykryte zdarzenie bezpieczeństwa, bez udziału operatora
Inwentaryzacja zasobów	Automatyczne budowanie i bieżąca aktualizacja inwentarza systemowego: zainstalowane aplikacje, uruchomione procesy, otwarte porty, informacje o sprzęcie i systemie operacyjnym
Monitorowanie kontenerów	Natywna integracja z silnikiem kontenerowym (Docker) umożliwiająca wykrywanie kontenerów działających w trybie uprzywilejowanym oraz z podatnymi aplikacjami
Integracja z usługami chmurowymi	Możliwość integracji z co najmniej jednym publicznym dostawcą chmury lub usługą pakietu biurowego (np. AWS, Microsoft Azure, GCP, Microsoft 365) w celu analizy zdarzeń bezpieczeństwa
Dashboardy i wizualizacja	Konfigurowalny, webowy interfejs do wyszukiwania, analizy i wizualizacji zebranych danych oraz zdarzeń bezpieczeństwa
Powiadomienia	Generowanie alertów w czasie rzeczywistym po wykryciu zdarzenia bezpieczeństwa, z możliwością powiadamiania e-mail oraz integracji z zewnętrznymi kanałami/systemami
Kontrola dostępu	Mechanizm kont i ról użytkowników z możliwością ograniczenia dostępu wybranym użytkownikom do określonych grup hostów/danych
Raportowanie zgodności	Generowanie raportów i widoków wspierających wykazanie zgodności z regulacjami/standardami bezpieczeństwa (np. PCI DSS, NIST, HIPAA)
Integracje / API	Otwarte REST API umożliwiające automatyzację, zarządzanie agentami oraz integrację z systemami zewnętrznymi
Skalowalność	Możliwość rozbudowy architektury (m.in. klastrowanie modułu zbierającego i indeksującego dane) w celu obsługi rosnącej liczby hostów i wolumenu danych, bez zmiany modelu licencyjnego

3. Rozszerzone wsparcie serwisowe

Parametr	Wymóg minimalny
Rozszerzone wsparcie serwisowe	System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub dystrybutora przez okres co najmniej do 31.12.2026 r., nie krócej jednak niż minimalny okres wsparcia nadawany natywnie przez producenta lub dystrybutora. System jest objęty usługą wsparcia technicznego świadczoną przez producenta, integratora lub Dystrybutora w języku polskim w zakresie: 1) Wsparcie telefoniczne zespołu certyfikowanych inżynierów. 2) Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. 3) Doradztwo w zakresie konfiguracji. 4) Zdalne wsparcie techniczne. 5) Pomoc w zakładaniu zgłoszeń serwisowych u producenta. 6) Przygotowanie do zdalnej konfiguracji. 7) Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. 8) Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. 9) Minimum dwa razy w roku opcjonalny zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. 10) Minimum dwa razy w roku opcjonalna zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wykonawca, na wezwanie Zamawiającego, przedłoży: 1) Oświadczenie Producenta lub Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

4. Oprogramowanie NAC z funkcją HoneyPot – licencja wieczysta na min. 50 urządzeń (adresów IP)

Opis funkcjonalności rozwiązania

Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).

Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez

administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.

Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.

Wymagania ogólne rozwiązania NAC

Lp.	Wymaganie
1	Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.
2	Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.
3	Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku nie spełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.
4	Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.
5	Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.
6	Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.
7	Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.
8	Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS
9	Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową
10	Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 50 urządzeń.
11	Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie co najmniej 50 urządzeń (adresów IP), wraz ze wsparciem technicznym producenta co najmniej do dnia 31.12.2026 r., nie krócej jednak niż minimalny okres wsparcia nadawany natywnie przez producenta wraz z licencją.

Wymagania szczegółowe – monitorowanie podsieci

Lp.	Wymaganie
1	Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.
2	Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora
3	Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie
4	Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.
5	Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.

Lp.	Wymaganie
6	Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane.
7	Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy

Wymagania szczegółowe – polityka bezpieczeństwa

Lp.	Wymaganie
1	Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.
2	W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.
3	Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci: a) pełny dostęp b) blokowanie (całkowity brak dostępu) c) ograniczony dostęp
4	Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.
5	Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.
6	Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.
7	Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.

Wymagania szczegółowe – mechanizm kwarantanny

Lp.	Wymaganie
1	Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa
2	Mechanizm kwarantanny powinien umożliwiać: a) całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, b) częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować
3	Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym, niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny
4	Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń
5	Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp

Lp.	Wymaganie
6	Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych
7	Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci
8	Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno

Wymagania szczegółowe – integracja z systemami zewnętrznymi

Lp.	Wymaganie
1	Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD
2	Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender lub z oprogramowaniem EDR/XDR dostarczanym w poz. 1.
3	Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-2, do definiowania polityki bezpieczeństwa.
4	Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie

Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)

Lp.	Wymaganie
1	Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.
2	Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.
3	Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory
4	Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń
5	Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych
6	Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci
7	W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy
8	Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu
9	Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa
10	Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci
11	Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu

Lp.	Wymaganie
12	Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych
13	Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.
14	Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant
15	Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant

Pozostałe wymagania

Lp.	Wymaganie
1	Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).
2	Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.
3	Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.
4	Rozwiązanie nie powinno pogarszać wydajności łączy WAN
5	Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci
Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalifikowanego inżyniera, certyfikowanego przez producenta rozwiązania: - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze - kwartalny przegląd konfiguracji rozwiązania Wykonawca, na wezwanie Zamawiającego, przedstawi: - oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia - osobowy certyfikat inżynierski pracownika, który będzie wykonywał wdrożenie

5. System IDS dla OT wraz z sondami sprzętowymi – 1 kpl. (oprogramowanie IDS + 5 szt. sond)

Przedmiotem zamówienia jest:

1) wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2) dostawa licencji oraz sond sprzętowych,
3) udzielenie wsparcia dla administratorów Zamawiającego,
4) organizacja i realizacja szkoleń dla administratorów Zamawiającego.

1. Funkcjonalność i specyfikacja

Lp.	Wymaganie
1	Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2	Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3	Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4	System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5	System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6	System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7	System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8	System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9	System IDS musi zapewniać: a) pasywne monitorowanie sieci przemysłowej Zamawiającego, b) automatyczne tworzenie graficznej mapy urządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach, c) szczegółową inwentaryzację urządzeń, d) automatyczne odzwierciedlenie połączeń komunikacyjnych, e) informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji, f) wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST, g) budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji, h) obsługę LLDP, CDP, CIP, SSDP.
10	System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11	System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12	System IDS musi mieć możliwość dodawania nowego typu protokołu.
13	System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14	Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników lub w trybie „pass-through / in-line" przy wpięciu do linii.
15	System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16	System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17	System IDS powinien być oparty na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18	System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19	System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog).
20	System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody/techniki behawioralne.

Lp.	Wymaganie
21	System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem ważności, typem, czasem wystąpienia.
22	System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23	System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24	System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25	System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC-61850, SRTP, BACnet.
26	System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27	System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowania działań naprawczych, rekomendacji.
28	System IDS musi wykrywać zagrożenia min.: a) malware, b) atak DOS/DDOS, c) atak typu APT, d) spyware, skanowanie sieci, e) zagrożenia Man-in-the-Middle, f) anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność komend, skanowanie PLC, skanowanie urządzeń sterujących, g) wykrywanie połączeń do innej sieci LAN/internet, h) wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.
29	System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30	System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31	System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32	System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33	System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34	System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BROADCAST.
35	System IDS musi mieć możliwość wykrywania producenta urządzenia min. po adresie MAC.
36	System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37	System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją, w której podsieci zostały one wykryte.
38	System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39	System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
40	Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
41	Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
42	Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.
43	Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44	Sonda sprzętowa musi być zabezpieczona przed ingerencją, tzn. dane muszą zostać skasowane przy próbie odczytu pamięci FLASH.
45	Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
46	Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.

Lp.	Wymaganie
47	Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
48	Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
49	Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
50	Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100 Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
51	Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazanej części ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
52	Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS strumienia sieciowego w formacie IPFIX.
53	System IDS musi współpracować z infrastrukturą sieciową Zamawiającego opartą na zaporach OPNsense, co najmniej w zakresie: a) przyjmowania kopii ruchu sieciowego z portów SPAN/mirror przełączników lub interfejsów w punktach styku sieci OT z zaporą.

2. Dostawa, wdrożenie

Lp.	Wymaganie
1	Wykonawca dostarczy: a) sondy sprzętowe w liczbie 5 szt. do monitorowania sieci przemysłowej, przeznaczone do instalacji w 5 obiektach wskazanych przez Zamawiającego, b) licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń, c) usługi wsparcia serwisowego producenta systemu IDS na okres od wdrożenia co najmniej do 31.12.2026 r., nie krócej jednak niż minimalny okres wsparcia nadawany natywnie przez producenta wraz z licencją. Serwis producenta systemu IDS ma obejmować: 1) dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim, 2) dostęp do nowych wersji systemu IDS, 3) dostęp do aktualizacji i poprawek systemu IDS, 4) dostęp do aktualizacji oprogramowania sond sprzętowych, 5) wymianę uszkodzonych sond sprzętowych w razie awarii, 6) przekazanie danych kontaktowych do działu technicznego producenta systemu IDS, 7) wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji, 8) wsparcie administratorów Zamawiającego przy identyfikacji problemów, a także ich rozwiązywaniu lub zastosowaniu obejścia.
1a	Licencja na system IDS musi być licencją bezterminową. Po upływie okresu wsparcia serwisowego system IDS oraz sondy sprzętowe muszą zachować pełną funkcjonalność w zakresie monitorowania, wykrywania i alarmowania, bez konieczności ponoszenia przez Zamawiającego dalszych opłat licencyjnych lub subskrypcyjnych.
2	Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
3	Licencje systemowe oraz sprzęt serwerowy zapewni Zamawiający.
4	Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający, a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw w działaniu sieci ani wprowadzać zakłóceń do sieci.
5	Wykonawca przeprowadzi pełną konfigurację i wdrożenie systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.

Lp.	Wymaganie
6	Wykonawca przekaże Zamawiającemu wszelkie hasła użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
7	Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
8	Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
9	Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.
10	Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

6. Oprogramowanie EDR dla OT – 5 licencji

Wymagania funkcjonalne oprogramowania EDR dla stacji operatorskich i serwerów w środowisku OT są tożsame z wymaganiami określonymi w poz. 1, z uwzględnieniem poniższych wymagań dodatkowych.

Parametr	Wymaganie minimalne
Liczba licencji	5 licencji na ochronę stacji operatorskich i serwerów w środowisku OT Zamawiającego.
Okres licencji i wsparcia	Licencja czasowa obejmująca okres od dnia aktywacji co najmniej do dnia 31.12.2026 r., nie krócej jednak niż minimalny okres licencji nadawany natywnie przez producenta, wraz z prawem do aktualizacji oprogramowania i baz zagrożeń oraz wsparciem technicznym producenta w tym okresie.
Zarządzanie	Zarządzanie z tej samej konsoli centralnej co licencje z poz. 1, z możliwością wydzielenia odrębnej grupy punktów końcowych OT z własnymi politykami ochrony.
Praca w sieci OT	Możliwość aktualizacji agentów i baz zagrożeń za pośrednictwem lokalnego punktu dystrybucji aktualizacji (serwer pośredniczący), bez konieczności zapewniania stacjom OT bezpośredniego dostępu do Internetu, oraz egzekwowanie polityk ochrony również przy braku łączności z konsolą.
Wpływ na proces technologiczny	Możliwość definiowania wykluczeń dla aplikacji i procesów systemów SCADA/HMI, skanowania z niskim priorytetem oraz kontroli harmonogramu skanowań i restartów, tak aby praca agenta nie wpływała na działanie systemów sterowania.
Integracja z SIEM	Przekazywanie zdarzeń bezpieczeństwa i incydentów do platformy SIEM dostarczanej w poz. 3.

Radosław Małysz

Elektronicznie podpisany przez Radosław Małysz
Data: 2026.10.21 11:23:05 +02'00'