

Załącznik nr 3d do SWZ

Szczegółowy opis przedmiotu zamówienia – część IV Systemy bezpieczeństwa

1. Oprogramowanie do backupu

Lp. Wymaganie

1. Model licencjonowania i dostawa

1.1 Oprogramowanie dostarczane w modelu licencji wieczystej (perpetual) — jednorazowa opłata licencyjna bez obowiązkowych opłat subskrypcyjnych; oprogramowanie pozostaje w użytkowaniu bezterminowo po zakończeniu okresu wsparcia

1.2 Licencja obejmuje prawo do użytkowania oprogramowania przez czas nieokreślony; aktualizacje i wsparcie techniczne dostępne opcjonalnie jako odrębna usługa odnawiana niezależnie od licencji

1.3 Możliwość rozszerzenia licencji (upgrade edycji lub dodanie licencjonowanych jednostek) bez konieczności ponownej instalacji lub migracji konfiguracji i zadań backupowych

1.4 Oprogramowanie wdrażane wyłącznie on-premise na infrastrukturze zamawiającego — bez przymusu korzystania z infrastruktury chmurowej producenta

1.5 W ramach zamówienia dostarczane: licencja na serwer backup (2 gniazda CPU hosta wirtualizacji) oraz licencja na backup stacji roboczych (40 stacji roboczych Windows/Linux)

2. Licencja — serwer backup maszyn wirtualnych

2.1 Licencja wieczysta per gniazdo procesora (CPU socket) hosta wirtualizacji — wymagana liczba licencji: 2 (dla serwera z dwoma gniazdami procesorowymi)

2.2 Licencja per socket nie ogranicza liczby maszyn wirtualnych chronionych na danym hoście — wszystkie VM działające na licencjonowanym hoście objęte ochroną w ramach jednej licencji

2.3 Licencja przenaszalna — możliwość przypisania do innego hosta wirtualizacji bez dodatkowych opłat

2.4 Obsługiwane platformy wirtualizacji: co najmniej Microsoft Hyper-V, VMware vSphere i Proxmox VE — licencja per socket wspólna dla wszystkich obsługiwanych platform

3. Licencja — backup stacji roboczych

3.1 Licencja wieczysta na backup fizycznych stacji roboczych — wymagana liczba: 40 stacji roboczych (licencje sprzedawane w pakietach po 5 sztuk; wymagane 8 pakietów)

3.2 Obsługiwane systemy operacyjne stacji roboczych: Windows 10/11 oraz dystrybucje Linux (Debian, Ubuntu, CentOS/RHEL lub równoważne)

3.3 Agent backupu stacji roboczych zarządzany z tej samej konsoli administracyjnej co backup maszyn wirtualnych — jeden interfejs dla całego środowiska

4. Funkcje backupu maszyn wirtualnych

4.1 Backup obrazowy maszyn wirtualnych (image-based, agentless) z wykorzystaniem mechanizmów snapshotów hypervisor — bez konieczności instalowania agenta wewnątrz VM

4.2 Backup inkrementalny oparty na śledzeniu zmienionych bloków (CBT — Changed Block Tracking) — minimalizacja okna backupowego i zużycia pasma

4.3 Granularne odzyskiwanie danych: możliwość przywrócenia pojedynczych plików lub folderów z backupu VM bez konieczności przywracania całej maszyny wirtualnej

4.4 Natychmiastowe uruchomienie VM (Instant VM Recovery) bezpośrednio z repozytorium backupu — minimalizacja czasu przestoju

4.5 Obsługa aplikacji świadomych VSS (Microsoft SQL Server, Active Directory, Exchange) — spójny backup na poziomie aplikacji

4.6 Replikacja maszyn wirtualnych do lokalizacji zapasowej (opcjonalnie) jako element strategii disaster recovery

5. Funkcje backupu stacji roboczych

5.1 Backup całego systemu stacji roboczej (bare metal / image-based) umożliwiający odtworzenie pełnego środowiska pracy użytkownika

5.2 Backup wybranych plików i folderów z możliwością definiowania harmonogramów i polityk retencji osobno dla każdej stacji lub grupy stacji

5.3 Granularne odzyskiwanie pojedynczych plików i folderów ze stacji roboczej bez konieczności przywracania całego obrazu systemu

5.4 Centralny monitoring statusu zadań backupu wszystkich stacji roboczych z poziomu konsoli administracyjnej

6. Bezpieczeństwo i ochrona danych

6.1 Szyfrowanie backupów algorytmem AES-256 — zarówno danych w repozytorium (at-rest), jak i podczas transmisji do repozytorium (in-transit); funkcja dostępna w ramach licencji bez dodatkowych opłat

- 6.2 Obsługa repozytoriów backupu z niezmiennością danych (immutability) — zabezpieczenie kopii zapasowych przed modyfikacją lub usunięciem przez ransomware lub nieautoryzowanego użytkownika
- 6.3 Obsługa rotacji nośników wymiennych (rotated drives) jako repozytorium backupu — umożliwiającą realizację strategii backupu 3-2-1 z kasetami RDX lub podobnymi nośnikami wymiennymi
- 6.4 Kontrola dostępu oparta na rolach (RBAC) — możliwość zdefiniowania różnych poziomów uprawnień dla administratorów i operatorów backupu
- 6.5 Uwierzytelnianie dwuskładnikowe (2FA) dla dostępu do konsoli administracyjnej
7. Wdrożenie i zarządzanie
- 7.1 Instalacja i zarządzanie wyłącznie on-premise — na serwerze zamawiającego z systemem Windows Server lub Linux; możliwość wdrożenia jako wirtualny appliance (OVF/OVA) na hoście wirtualizacji
- 7.2 Interfejs zarządzania dostępny przez przeglądarkę internetową (HTTPS) bez konieczności instalowania dedykowanego klienta na stacjach administratora
- 7.3 Automatyczne harmonogramowanie zadań backupu z możliwością definiowania okien backupowych, polityk retencji i reguł powiadamiania
- 7.4 Powiadomienia e-mail o statusie zadań backupu (sukces, ostrzeżenie, błąd) z możliwością integracji z z z SMTP zamawiającego
- 7.5 Obsługa deduplikacji i kompresji danych w repozytorium — redukcja zajętości przestrzeni dyskowej przez kopie zapasowe
- 7.6 Możliwość weryfikacji integralności kopii zapasowych (backup verification) — automatyczne testowanie możliwości odtworzenia danych bez ingerencji administratora
8. Wsparcie techniczne i aktualizacje
- 8.1 W ramach zamówienia: 12 miesięcy wsparcia technicznego producenta w dni robocze (Standard Support) — od daty dostarczenia licencji
- 8.2 W okresie aktywnego wsparcia: dostęp do aktualizacji oprogramowania (poprawki bezpieczeństwa i nowe wersje) bez dodatkowych opłat
- 8.3 Po wygaśnięciu wsparcia: możliwość dalszego użytkowania oprogramowania w posiadanej wersji bez żadnych dodatkowych opłat; odnowienie wsparcia opcjonalne i niezależne
- 8.4 Oprogramowanie dystrybuowane przez autoryzowanego partnera lub dystrybutora producenta na terenie Polski; oferent zobowiązany do przedłożenia oświadczenia potwierdzającego autoryzację

2. EDR Endpoint Detection and Response (40 sztuk)

ZAPOBIEGANIE I WYKRYWANIE

Funkcjonalność	Implementacja
Rozwiązanie musi wykrywać złośliwe pliki i zapobiegać ich wykonaniu, w tym wirusy, trojany, ransomware, spyware, kryptominery i inne rodzaje złośliwego oprogramowania.	Ochrona przed złośliwym oprogramowaniem oparta na sygnaturach Statyczna analiza z użyciem uczenia maszynowego Dynamiczna analiza (sandbox w czasie rzeczywistym) Dane wywiadowcze o zagrożeniach (VirusTotal) Threat Intelligence (inne źródła niż VT) Integracja z Microsoft Windows AMSI (Antimalware Scan Interface)
Rozwiązanie musi wykrywać złośliwe zachowania uruchomionych plików, procesów, modyfikacji rejestru i dostępu do pamięci oraz zatrzymywać je w czasie rzeczywistym lub generować alert (np. exploits, fileless, makra, Powershell, WMI itp.).	Monitorowanie dostępu do pamięci Analiza zachowania procesów (heurystyka) Wysokie podobieństwo (tzw. fuzzy hashing) Dane wywiadowcze o zagrożeniach
Rozwiązanie musi umożliwiać tworzenie reguł ostrzegających komunikacji z określonymi adresami IP	Czarna lista złośliwych adresów IP i domen
Rozwiązanie musi wykrywać i blokować ataki polegające na eskalacji uprawnień.	Monitorowanie procesów
Rozwiązanie musi wykrywać i blokować ataki rozpoznawcze (skanowanie).	Analiza ruchu w sieci
Rozwiązanie musi wykrywać i blokować próby kradzieży z pamięci (zrzuty haseł, brute force) lub z ruchu sieciowego (spoofing, DNS Responder).	Monitorowanie pamięci Monitorowanie kont użytkowników (próby logowania) Analiza zachowań w ruchu sieciowym
Rozwiązanie musi wykrywać i blokować (lub ostrzegać) o próbach bocznego (np. SMB relay, pass-the-hash).	Monitorowanie ruchu w sieci. Wprowadzenie w błąd poprzez fałszywe węzły. Wprowadzenie w błąd poprzez fałszywe konta użytkowników.

	Nprowadzenie w błąd poprzez fałszywe połączenia sieciowe.
Rozwiązanie musi wykrywać złośliwe zachowanie kont użytkowników, wskazujące na wcześniejsze naruszenie bezpieczeństwa.	<p>konfigurowanie zasad aktywności użytkownika (naruszenie polityki).</p> <p>Profilowanie bazowego zachowania konta użytkownika (wykrywanie anomalii).</p>
Rozwiązanie musi wykrywać złośliwą interakcję z plikami danych.	Nprowadzenie w błąd za pomocą plików pułapek.
Rozwiązanie musi wykrywać wyciek danych przy użyciu legalnych protokołów (tunneling DNS, tunneling ICMP).	<p>Monitorowanie ruchu w sieci.</p> <p>Monitorowanie dostępu do plików.</p>
Rozwiązanie musi wykrywać i blokować użycie popularnych narzędzi do ataków (Metasploit, Empire, Cobalt itd.).	Monitorowanie procesów.
Rozwiązanie musi zawierać mechanizm wewnętrznej ochrony przed alarmuj i blokuj każdą próbę manipulacji lub wyłączenia.	
Rozwiązanie musi umożliwiać wykrywanie i blokowanie komunikacji z złośliwymi domenami.	<p>Filtrowanie nazw domen</p>
DOCHODZENIE I USUWANIE ZAGROŻEŃ	
Rozwiązanie musi stale zbierać dane o wszystkich podmiotach i ich działaniach w środowisku.	<p>interakcje z plikami tworzenie, otwieranie, zmiana nazwy, usuwanie, uruchamianie</p> <p>Wykonywanie procesów (w tym drzewo procesów)</p> <p>Logowanie użytkownika</p> <p>Ruch sieciowy</p> <p>Zmiany w rejestrze</p> <p>Zainstalowane oprogramowanie</p>
Rozwiązanie musi wspierać wyświetlanie danych o podmiotach i ich aktywności.	<p>Nyszukiwanie oparte na wzorcach zachowań we wszystkich obszarach (użytkownicy, pliki, maszyny, ruch sieciowy).</p> <p>Określenie reguł i/lub tworzenie ostrzeżeń i/lub określenie poziomu ryzyka w oparciu o wzorzec wyszukiwania w czasie rzeczywistym.</p> <p>Możliwość wykonywania działań równolegle przez wielu użytkowników, zgodnie z ich uprawnieniami, bez potrzeby rozłączania innych użytkowników.</p>
Rozwiązanie musi wspierać analizę dynamiczną (np. sandbox).	Ręczne przesyłanie plików do analizy w sandboxie.
Rozwiązanie musi wspierać zapytania międzyorganizacyjne.	Nyszukiwanie występowania procesów/plików/ruchu sieciowego/aktywności użytkowników na wszystkich punktach końcowych w środowisku.
Rozwiązanie musi wspierać prowadzenie dochodzenia kryminalistycznego.	<p>Uruchomiony proces/plik.</p> <p>Poziom maszyny.</p> <p>Aktywność pamięci.</p> <p>Pobieranie zrzutu pamięci.</p>
Rozwiązanie musi wspierać izolowanie i eliminowanie złośliwej aktywności lokalnie na punkcie końcowym.	<p>Możliwość uruchomienia skoordynowanego polecenia (np. interfejs CMD).</p> <p>Uruchamianie skryptu lub pliku z zasobu sieciowego lub mapowanie dysku.</p> <p>Nyłączenie punktu końcowego i/lub serwera.</p> <p>zoliczanie punktu końcowego/serwera od sieci.</p> <p>Jsunięcie pliku (w tym uruchomionego pliku).</p> <p>Przeniesienie pliku do kwarantanny (w tym uruchomione pliki).</p> <p>Zakończenie procesu.</p> <p>Jsunięcie lub skasowanie usługi/zaplanowanego zadania.</p> <p>Zablokowanie lokalnego konta użytkownika lub użytkownika domenowego.</p> <p>Nyzerowanie hasła użytkownika.</p> <p>3blokowanie komunikacji na podstawie adresu docelowego (domena lub adres IP).</p> <p>Odłączenie kart sieciowych.</p> <p>Zmiana adresu IP</p> <p>Możliwość edytowania pliku HOSTS.</p> <p>onowne uruchomienie punktu końcowego i/lub serwera.</p>

Rozwiązanie musi wspierać izolowanie i usuwanie złośliwej obecności i aktywności w całym środowisku.

Rozwiązanie musi wspierać automatyzację reakcji.

Rozwiązanie musi zawierać automatyczny mechanizm badania wykrytych incydentów bezpieczeństwa oraz możliwość samodzielnego ich usuwania.

Rozwiązanie musi pokazywać łańcuch zdarzeń i powiązane obiekty, które doprowadziły do incydentu.

MONITOROWANIE I KONTROLA

Funkcjonalność

Rozwiązanie musi obsługiwać monitorowanie integralności plików (FIM).

Rozwiązanie musi mieć wbudowane mechanizmy oceny podatności.

Rozwiązanie musi umożliwiać prowadzenie zarządzania zasobami.

Rozwiązanie musi umożliwiać zbieranie i przechowywanie logów.

Rozwiązanie musi umożliwiać polowanie na zagrożenia (threat hunting).

Rozwiązanie musi wspierać wykrywanie niechronionych powierzchni ataku.

Active Directory: dezaktywacja użytkownika, resetowanie hasła

Firewall/proxy: blokada IP, domeny lub portu.

Gotowe scenariusze odpowiedzi dostępne w ramach rozwiązania.

Scenariusze odpowiedzi dostosowane przez operatora.

Badanie: umożliwia identyfikację trwałych zagrożeń, przyczyn źródłowych i naruszonych elementów w całej chronionej infrastrukturze.

Usuwanie: automatyczne eliminowanie złośliwych elementów wykrytych podczas fazy badania.

Wizualizacja graficzna incydentu, pokazująca zdarzenia i dane dotyczące ofiary, sprawcy oraz powiązania między artefaktami danych a pełnym drzewem procesów i łańcuchem zdarzeń.

Implementacja

Wymuszanie zasad w środowiskach stałych w celu ostrzegania o wszelkich zmianach w plikach.

Wykrywanie brakujących aktualizacji zabezpieczeń w systemach i aplikacjach.

Mapowanie i korelowanie wszystkich zasobów w środowisku, takich jak punkty końcowe, serwery, zainstalowane aplikacje, konta użytkowników oraz generowanie okresowych raportów.

Zbieranie logów uwierzytelniania i aktywności oraz ich przechowywanie przez okres wymagany przez odpowiednie regulacje.

Wyszukiwanie obecności zagrożeń na podstawie znanych wskaźników kompromitacji (IOC).

Wyszukiwanie plików, procesów, połączeń sieciowych i kont użytkowników z niezmienionymi hasłami, podatnych na ryzyko.

INFRASTRUKTURA

Funkcjonalność

Rozwiązanie musi oferować elastyczne opcje wdrażania serwerów, dopasowane do różnych typów środowisk

Rozwiązanie musi wspierać szybkie i bezproblemowe wdrożenie na wszystkich punktach końcowych/serwerach w środowisku.

Rozwiązanie musi obsługiwać automatyczną dystrybucję na punktach końcowych/serwerach dodanych do środowiska po początkowej instalacji.

Rozwiązanie musi mieć niewielki wpływ na wydajność punktu końcowego/serwera.

Implementacja

W środowisku lokalnym (on-premise)

SaaS (model usługi)

Tryb hybrydowy

Wymagany czas wdrożenia na 5000 punktach końcowych.

Autonomiczne wykrywanie nowych maszyn i instalacja agenta bez konieczności ręcznej konfiguracji.

~50 MB pamięci RAM wykorzystywanej na każdym punkcie końcowym/serwerze.

~2–5% zasobów CPU zużywanych na każdej platformie punktu końcowego.

Rozwiązanie musi zapewniać szyfrowaną komunikację między serwerem zarządzającym a agentami na punktach końcowych/serwerach.

Rozwiązanie musi obsługiwać wszystkie powszechnie używane systemy operacyjne.

Systemy zakończone wsparciem: Windows XP/Vista, Server 2003

Windows 7 i nowsze

Windows Server 2008 R2 i nowsze

Główne dystrybucje Linuksa: Fedora, Ubuntu, Debian, CentOS, Red Hat, Suse, Oracle, Alma, Amazon macOS 10.15 Catalina i nowsze (Intel i Apple Silicon)

Rozwiązanie musi obsługiwać połączenie z Active Directory.	Szczegółowa autoryzacja do interfejsu użytkownika. Wdrażanie do różnych grup OU w AD.
Rozwiązanie musi umożliwiać definiowanie ról administracyjnych z niestandardowymi uprawnieniami.	Tworzenie ról z dostosowanymi uprawnieniami na podstawie typów dostępnych działań przypisywanych użytkownikom lokalnym, grupom i użytkownikom AD.
Rozwiązanie musi współistnieć z ogólnodostępnym i własnościowym oprogramowaniem na punktach końcowych\serwerach.	Bezproblemowe działanie chronionego punktu końcowego/serwera bez błędów typu BSOD lub awarii procesów.
Rozwiązanie musi zapewniać pełną ochronę punktów końcowych i serwerów pracujących offline poza siecią organizacji.	Mechanizmy ochrony przed zagrożeniami niezależne od połączenia z serwerem zarządzania.
Rozwiązanie musi autonomicznie zbierać dane o punktach końcowych, plikach, procesach, aktywności użytkowników i ruchu sieciowym.	Eliminacja potrzeby ręcznej konfiguracji reguł, polityk lub wykorzystania dodatkowych urządzeń.
OPERACJE	
Rozwiązanie musi umożliwiać określenie listy wykluczeń dla wybranych obiektów.	
Rozwiązanie musi obsługiwać wdrażanie na wielu lokalizacjach raportujących do jednej konsoli zarządzania.	
Rozwiązanie musi umożliwiać eksport aktualnej konfiguracji programu w celu późniejszego importu na tym samym lub innym komputerze.	
Rozwiązanie musi umożliwiać włączanie/wyłączanie określonych typów powiadomień.	
Rozwiązanie musi umożliwiać ocenę poziomu zagrożenia w alertach bezpieczeństwa.	
Rozwiązanie musi zapewniać centralne zbieranie i przetwarzanie alertów w czasie rzeczywistym.	
Rozwiązanie musi umożliwiać blokowanie dostępu do ustawień programu dla użytkowników końcowych.	
Rozwiązanie musi zapewniać centralną dystrybucję aktualizacji bez potrzeby interwencji użytkownika i bez konieczności ponownego uruchamiania punktów końcowych/serwerów.	
Rozwiązanie musi umożliwiać określenie harmonogramu pobierania aktualizacji, w tym możliwość wyłączenia automatycznych aktualizacji.	
Rozwiązanie musi przypisywać ocenę ryzyka wszystkim obiektom w chronionym środowisku.	
Rozwiązanie musi obsługiwać rejestrowanie zdarzeń, alertów i aktualizacji.	
Rozwiązanie musi umożliwiać wydłużenie domyślnego okresu przechowywania danych, aby zrównoważyć prywatność i polityki firmowe.	
Rozwiązanie musi obsługiwać integrację z infrastrukturą e-mail w celu powiadamiania personelu ds. bezpieczeństwa o alertach.	
Rozwiązanie musi obsługiwać integrację z popularnymi systemami SIEM (za pomocą logów syslog, API i plików JSON wysyłanych do AWS S3; zarówno dla alertów, jak i logów audytowych).	
Rozwiązanie musi umożliwiać pobieranie logów syslog zewnętrznych dostawców i centralizację ich w jednym widoku (logi muszą być widoczne jako dane surowe lub przedstawione na wykresach w różnych formach).	
Rozwiązanie musi obsługiwać raporty standardowe i konfigurowalne. Raporty muszą być eksportowalne w różnych formatach, możliwe do zaplanowania i wysyłane e-mailem.	
Rozwiązanie musi oferować aplikację na smartfony, smartwatche i tablety, która pokazuje liczbę chronionych zasobów, liczbę otwartych alarmów, nowe alarmy wraz z ich typem, wpływem, poziomem zagrożenia i reakcją oraz umożliwia bezpośrednie zaangażowanie zespołu SOC w celu rozpoczęcia dochodzenia.	
WYMOGI DOTYCZĄCE SKUTECZNOŚCI	
(Potwierdzone przez wynik testów MITRE ATT&CK Evaluation)	
Przynajmniej 1	
Rozwiązanie zablokowało wszystkie 10 technik ataku w scenariuszu Protections w ewaluacji Enterprise 2025	
Liczba niewykrytych podtechnik (oznaczonych na żółto) w stosunku do wszystkich podtechnik (21) nie może przekraczać 5% w scenariuszu Protections w ewaluacji Enterprise 2024.	
USŁUGI, WSPARCIE I SLA	
Szkolenie: Dostawca musi zapewnić co najmniej 2 dni szkolenia: na miejscu albo zdalnie (do uzgodnienia)	
TAM (Technical Account Manager): Dostawca musi w ramach licencji zapewnić Menedżera Technicznego Konta, który przynajmniej raz w miesiącu zapewni wsparcie, optymalizację i konsultacje.	
Usługa wsparcia (Wymagane SLA zaznaczyć w ofercie dostawcy):	
Krytyczny: Krytyczny problem produkcyjny znacznie wpływający na korzystanie z usługi. Brak obejścia proceduralnego. (np.: problem uniemożliwiający całkowicie korzystanie z oprogramowania). Wymagane SLA: 2 godziny.	
Wysoki: Poważna degradacja wydajności lub funkcjonalności aplikacji (np.: problem uniemożliwiający aktualizację do najnowszej wersji). Wymagane SLA: 6 godzin	
Normalny: Problem z aplikacją o umiarkowanym wpływie na działalność (np.: błąd uniemożliwiający użycie funkcji). Wymagane SLA: 2 dni robocze	
Niski: Problem lub pytanie o niewielkim wpływie na działalność (np.: pytanie techniczne lub problem z GUI, który nie uniemożliwia pracy). Wymagane SLA: 3 dni robocze	

Technologia musi być uzupełniona przez usługę MDR działającą 24/7, niezależnie od wielkości i kompetencji zespołu ds. bezpieczeństwa. Usługa ta ma monitorować, analizować i wspierać zarządzanie alertami o wysokim i krytycznym poziomie. SLA dla tej usługi MDR to:

Krytyczny 2 godziny

Wysoki 4 godziny

DODATKOWE MODUŁY PLATFORMY

Identyfikowanie, automatyczne priorytetyzowanie i korygowanie zagrożeń bezpieczeństwa w aplikacjach SaaS lub monitorowanej infrastrukturze chmurowej bezpośrednio z poziomu oferowanej platformy.

Monitorowanie, analizowanie i korelowanie kluczowych działań wykonywanych w środowisku korporacyjnym poprzez wykorzystanie istniejących logów, skoncentrowanych w scentralizowanej platformie zarządzania logami z możliwością przeszukiwania i wizualizacji analitycznej.

Monitorowanie niezamierzonego wystawienia usług poprzez obecność publicznie dostępnych usług firmowych (domeny publiczne lub adresy IP).

Monitorowanie dark webu, w szczególności w zakresie kradzieży danych uwierzytelniających.

Identyfikowanie, automatyczne priorytetyzowanie i korygowanie znanych luk (CVE) i błędnych konfiguracji na punktach końcowych bezpośrednio z poziomu oferowanej platformy.

Dodatkowe zabezpieczenie poczty e-mail

Obsługa integracji poprzez własne API oraz wykorzystanie API stron trzecich.

Udostępnianie comiesięcznego raportu zagrożeń zawierającego najnowsze trendy i statystyki dotyczące poważnych ataków, co zapewnia kluczowe informacje potrzebne do utrzymania bezpieczeństwa.

Ochrona urządzeń mobilnych z systemami Android, iOS i ChromeOS będzie oceniana pozytywnie. W szczególności jeśli ochrona dotyczy samego systemu operacyjnego urządzenia, połączeń sieciowych, zachowań aplikacji i phishingu; Nawet jeśli polityki bezpieczeństwa dla urządzeń mobilnych są inne i zarządzane z osobnej konsoli, to logi zagrożeń i audytu muszą być zintegrowane z oferowaną platformą XDR.

Ochrona skrzynek pocztowych

Wymagane jest rozwiązanie ochrony przed naruszeniami w formie samodzielnej platformy, która natywnie integruje wykrywanie i zapobieganie atakom w sieci, na użytkownikach i punktach końcowych z automatycznym dochodzeniem i reakcją w całej infrastrukturze wszystko za pośrednictwem jednego lekkiego agenta, bez dodatkowego nakładu operacyjnego.

3. Antywirus antymalware (40 sztuk)

Parametr	Opis i funkcjonalność
Typ rozwiązania	Wielowarstwowe oprogramowanie antywirusowe klasy EPP (Endpoint Protection Platform), przeznaczone do ochrony stacji roboczych i serwerów w środowiskach firmowych. Może stanowić integralną część EDR/XDR.
Zakres licencji	<p>licencja subskrypcyjna na 40 urządzeń:</p> <p>40 stacji roboczych (Windows/macOS/Linux)</p> <p>2 serwery (Windows Server/Linux Server)</p> <p>licencja obejmuje pełne wsparcie techniczne, aktualizacje sygnatur, dostęp do konsoli zarządzającej i wszystkich funkcji ochrony.</p>
Silnik ochrony	<p>Nykrywanie zagrożeń w czasie rzeczywistym</p> <p>Wbudowany silnik heurystyczny i behawioralny</p> <p>Chmurowa analiza reputacji</p> <p>Nykrywanie zagrożeń typu fileless, exploitów, rootkitów i</p> <p>3aza sygnatur: liczona w milionach znanych zagrożeń aktualizowanych codziennie</p>
Ochrona przed ransomware	<p>Moduł analizujący zachowanie aplikacji i blokujący działania typowe dla ransomware</p> <p>Możliwość działania w trybie audytu</p> <p>Zdalna konfiguracja z poziomu konsoli zarządzającej</p>
Funkcja Rollback	<p>Możliwość przywrócenia plików zaszyfrowanych przez ransomware (jeśli system plików i konfiguracja na to pozwalają)</p> <p>Integracja z lokalnymi punktami przywracania systemu.</p> <p>Żgodność z wytycznymi NIST dotyczącymi odzyskiwania po ataku ransomware</p>
Zarządzanie	<p>Konsola zarządzająca dostępna w wersji lokalnej (on-premise) lub chmurowej</p> <p>Zarządzanie politykami, grupami, zadaniami, aktualizacjami i raportami</p> <p>Integracja z Active Directory i synchronizacja użytkowników</p> <p>Obsługa wielu lokalizacji i administratorów</p>
Zarządzanie podatnościami	Możliwość rozszerzenia o moduł zarządzania poprawkami aktualizacje systemu Windows i aplikacji firm trzecich (np. Java, Adobe, Zoom).
Raportowanie powiadomienia	<p>ponad 170 gotowych szablonów raportów</p> <p>Możliwość tworzenia własnych raportów z ponad 1000 zmiennych</p> <p>powiadomienia e-mail, webhooki, alerty konfigurowalne przez edytor typu WYSIWYG</p>

Instalacja i wdrożenie	Instalatory prekonfigurowane
	Automatyczne przypisywanie urządzeń do instancji i subskrypcji
	Masowa instalacja przez AD, GPO, skrypty lub linki instalacyjne
Szkolenie	Wymagane szkolenie administratorów w języku polskim, obejmujące: konfigurację konsoli, polityk i grup na incydenty
	reagowanie na incydenty
	zarządzanie aktualizacjami i raportowaniem
	integrację z AD i scenariusze DR
Wsparcie techniczne	Wsparcie techniczne w języku polskim (min. 8/5) oraz angielskim (24/7)
	Dostęp do portalu klienta, systemu zgłoszeń, aktualizacji i dokumentacji
	Możliwość kontaktu telefonicznego, e-mailowego i przez chat
Gwarancja	Licencja na min. 36 miesięcy
utrzymanie	Gwarancja działania zgodnie z dokumentacją producenta
	Dostęp do aktualizacji sygnatur, silników i poprawek bezpieczeństwa
Zgodność i certyfikaty	Zgodność z RODO, ISO 27001, ENISA
	Certyfikaty niezależnych laboratoriów testujących oprogramowanie zabezpieczające
	Możliwość wdrożenia w środowiskach o podwyższonym poziomie bezpieczeństwa (np. sektor publiczny, finansowy)
Pakiet z EDR	Antywirus może stanowić część pakietu EDR/XDR po uzgodnieniu z Zamawiającym.

4. Organizacja realizacji zamówienia

- Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
- Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiającego nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
- Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
- Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
- Jakiegokolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyko problemów.
- Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z każdym z Zamawiających. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
- Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
- Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w zapytaniu ofertowym i nie są z nimi sprzeczne.
- Zamawiający we współpracy z Wykonawcą ustalą harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
- Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.
- W niniejszym dokumencie opisano wymagania minimalne.

5. Wdrożenie

- Każdy z systemów stanowiący przedmiot dostawy winien zostać wdrożony w sposób umożliwiający prawidłowe funkcjonowanie bez negatywnego wpływu na środowisko Zamawiającego.
- W przypadku dostawy rozwiązania opierającego się o serwer Wykonawca wdroży je w całości na serwerze oraz w 40% na urządzeniach/użytkownikach objętych wdrożeniem.
- Wdrożenie ma odbywać się wraz z Zamawiającym co oznacza, że Wykonawca będzie prowadził prace bezpośrednio w obecności Zamawiającego.