

Część 8 – Oprogramowanie antywirusowe z funkcjami XDR, szyfrowania danych, uwierzytelnienia dwuskładnikowego

I. Charakterystyka ogólna i cel zamówienia

Przedmiotem zamówienia jest dostawa subskrypcji licencyjnych w ramach wznowienia i rozbudowy (Upgrade) obecnie posiadanego przez Zamawiającego systemu zabezpieczeń. Zamawiający używa obecnie oprogramowanie **ESET PROTECT Essential On-Prem** (licencje ważne do 2026-04-28). Celem postępowania jest podniesienie standardu bezpieczeństwa do poziomu funkcjonalnego odpowiadającego pakietowi **ESET PROTECT Elite** (lub rozwiązaniu równoważnemu) oraz migracja środowiska zarządzającego z infrastruktury lokalnej do chmury producenta.

Nowa subskrypcja musi obejmować licencje dla **85** urządzeń i obowiązywać przez okres **12 miesięcy** od daty aktywacji. Rozwiązanie musi zapewniać kompleksową ochronę stacji roboczych, serwerów plików, urządzeń mobilnych oraz usług chmurowych, wzbogaconą o zaawansowane mechanizmy detekcji i reagowania (XDR), szyfrowanie danych, zarządzanie podatnościami oraz uwierzytelnianie wieloskładnikowe.

II. Architektura rozwiązania i zarządzanie centralne

System musi funkcjonować w modelu **SaaS (Software as a Service)**, co oznacza, że konsola zarządzająca utrzymywana jest w chmurze producenta, eliminując konieczność posiadania przez Zamawiającego własnych serwerów zarządzających. Dostęp do konsoli musi odbywać się poprzez przeglądarkę internetową, zabezpieczoną protokołem SSL/TLS, z wymuszeniem uwierzytelniania dwuskładnikowego (2FA) dla kont administratorów.

Platforma zarządzająca musi umożliwiać pełną administrację politykami bezpieczeństwa, zadaniami oraz licencjami. Wymagana jest funkcjonalność tworzenia dynamicznych grup urządzeń, które automatycznie sortują komputery na podstawie spełnionych kryteriów (np. wersja systemu, stan zagrożenia, adres IP). System musi posiadać mechanizm automatyzacji zadań (Task Scheduler) oraz obsługiwać komunikację agentów poprzez HTTP Proxy. W celu zapewnienia rozliczalności działań, konsola musi oferować system nadawania uprawnień (RBAC) oraz generowania zaawansowanych raportów z możliwością ich automatycznej wysyłki.

III. Kompleksowa Ochrona Stacji Roboczych (Endpoint Security)

1. Wielowarstwowy silnik ochrony i wspierane platformy System ochrony punktów końcowych musi zapewniać pełne wsparcie dla heterogenicznego środowiska informatycznego, obejmującego stacje robocze z systemami Microsoft Windows (wersje 10 i 11, w tym architektura ARM64), macOS (wersja 11 Big Sur i nowsze, z natywną obsługą architektury Apple Silicon/ARM) oraz Linux Desktop (Ubuntu, RHEL, Linux Mint 64-bit). Silnik antywirusowy musi wykorzystywać wielowarstwową technologię detekcji, łączącą klasyczne sygnatury z zaawansowaną heurystyką pasywną i aktywną oraz elementami sztucznej inteligencji (uczenie maszynowe). Wymagana jest głęboka integracja sprzętowa – rozwiązanie musi współpracować z technologią **Intel Threat Detection Technology (TDT)**, wykorzystując telemetrię z procesora do wykrywania zaawansowanych zagrożeń, w tym złośliwego oprogramowania ukrywającego się przed systemem operacyjnym.

2. Ochrona przed Ransomware i Botnetami Rozwiązanie musi posiadać dedykowany moduł ochrony przed oprogramowaniem wymuszającym okup (**Ransomware Shield**), który

Załącznik nr 1.8

monitoruje i ocenia zachowanie uruchomionych aplikacji. W przypadku wykrycia próby nieautoryzowanego szyfrowania plików, system musi zablokować proces oraz umożliwić przywrócenie zaszyfrowanych plików. Dodatkowo wymagana jest ochrona przed botnetami, blokująca komunikację stacji z serwerami C&C (Command & Control) oraz wbudowana technologia ochrony przed rootkitami i atakami typu backdoor.

3. Ochrona Sieci, Poczty i Przeglądarki (Secure Browser) System musi zapewniać bezpieczeństwo na poziomie sieciowym poprzez zaporę ogniową (Firewall) pracującą w jednym z czterech trybów: automatycznym, interaktywnym, opartym na regułach lub trybie uczenia się. Rozwiązanie musi skanować ruch sieciowy wewnątrz szyfrowanych protokołów HTTPS, POP3S oraz IMAPS, a także oczyszczać pocztę „w locie” (niezależnie od klienta pocztowego). Dla zapewnienia bezpieczeństwa transakcji finansowych, system musi być wyposażony w moduł **Bezpiecznej Przeglądarki**, która automatycznie szyfruje znaki wprowadzane z klawiatury, chroniąc przed keyloggerami (praca w tym trybie musi być wizualnie wyróżniona np. kolorową ramką). Rozwiązanie musi również umożliwiać kontrolę dostępu do stron WWW (Web Control) w oparciu o minimum 140 predefiniowanych kategorii tematycznych.

4. Kontrola Urządzeń i System HIPS Rozwiązanie musi zapewniać granularną kontrolę dostępu do portów i urządzeń peryferyjnych (Device Control). Administrator musi mieć możliwość blokowania lub dopuszczania (w trybie tylko do odczytu) nośników takich jak: pamięci USB, dyski FireWire, napędy optyczne, urządzenia Bluetooth oraz czytniki kart, w oparciu o reguły uwzględniające typ urządzenia, jego numer seryjny, producenta lub model. Kluczowym elementem ochrony behawioralnej musi być system zapobiegania włamaniom działający na hoście (**HIPS**), pracujący w jednym z pięciu trybów:

- a. **Automatyczny z regułami:** wykorzystujący reguły producenta i użytkownika.
- b. **Interaktywny:** pytający użytkownika o decyzję.
- c. **Oparty na regułach:** blokujący wszystko, co nie jest dozwolone.
- d. **Tryb uczenia się:** automatycznie tworzący reguły na podstawie obserwacji ruchu przez określony czas.
- e. **Tryb inteligentny:** powiadamiający tylko o zdarzeniach szczególnie podejrzanych.

5. Diagnostyka i Ochrona Mobilna (Android) Agent na stacji roboczej musi posiadać narzędzie diagnostyczne generujące pełny raport o stanie systemu (procesy, usługi, sterowniki, rejestr), umożliwiające filtrowanie wyników pod kątem poziomu ryzyka (min. 9 poziomów). W zakresie ochrony urządzeń mobilnych z systemem Android, rozwiązanie musi oferować skanowanie w czasie rzeczywistym i na żądanie (pamięć wewnętrzna i karty SD), kontrolę aplikacji (blokowanie wg uprawnień, kategorii Google Play lub źródła pochodzenia) oraz funkcje Anti-Theft: zdalne czyszczenie, blokada, lokalizacja GPS, sygnał dźwiękowy i weryfikacja zaufanej karty SIM.

IV. Zaawansowana Ochrona Serwerów (Server Security)

Wymagana jest dedykowana ochrona dla serwerów pracujących pod kontrolą systemów Microsoft Windows Server (2012–2025) oraz Linux. Rozwiązanie musi być zoptymalizowane pod kątem środowisk wirtualnych (VMware/Hyper-V) poprzez zastosowanie mechanizmu współdzielonej pamięci podręcznej (np. Shared Local Cache), co eliminuje wielokrotne skanowanie tych samych plików na różnych maszynach wirtualnych i zapobiega spadkom wydajności hosta.

Załącznik nr 1.8

Agent serwerowy musi automatycznie rozpoznawać role serwera (np. Active Directory, SQL, IIS, Exchange) i samoczynnie konfigurować zalecane wykluczenia ze skanowania. Ochrona musi obejmować monitorowanie procesów w pamięci RAM (integracja z AMSI) w celu wykrywania ataków bezplikowych (*fileless malware*) oraz ochronę usług sieciowych (RDP, SMB) przed atakami typu Brute-Force. W przypadku serwerów Linux wymagane jest udostępnienie interfejsu graficznego (WebGUI) dostępnego przez przeglądarkę.

V. Moduły Rozszerzone: Cloud Sandbox, Ochrona Usług Chmurowych i Zarządzanie Podatnościami

1. Analiza 0-day w Chmurze (Cloud Sandbox) W celu ochrony przed nieznanymi zagrożeniami (Zero-Day), system musi posiadać funkcjonalność automatycznego przesyłania podejrzanych próbek do chmury producenta (Cloud Sandbox). Mechanizm ten musi obejmować pliki wykonywalne, skrypty, instalatory, dokumenty oraz archiwa. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanej próbki, czasu jej przechowywania oraz wykluczeń (np. dla konkretnych folderów). Kluczową wymaganą funkcjonalnością jest **proaktywna blokada**: w przypadku stacji roboczych system musi wstrzymać uruchomienie pobranego pliku, a w przypadku serwerów pocztowych wstrzymać dostarczenie wiadomości e-mail do momentu zakończenia analizy w chmurze i otrzymania werdyktu (Czysty, Podejrzany, Szkodliwy). Wynik analizy musi być automatycznie współdzielony ze wszystkimi chronionymi stacjami w organizacji.

2. Ochrona Usług Chmurowych (Cloud Office Security) System musi zapewniać natywną ochronę (API) dla środowisk **Microsoft 365** (Exchange Online, OneDrive, SharePoint, Teams) oraz **Google Workspace** (Gmail, Google Drive), z obsługą wielu tenantów w jednej konsoli. W zakresie ochrony poczty (Exchange/Gmail), rozwiązanie musi oferować zaawansowany filtr antyspamowy i antyphishingowy, wykorzystujący mechanizmy SPF, DKIM, DMARC oraz reputację nadawcy. Konsola zarządzająca musi raportować użytkowników najbardziej narażonych na ataki (Top Spam/Phishing/Malware Receivers). Dla usług dyskowych (OneDrive/SharePoint/Teams), system musi skanować pliki pod kątem złośliwego oprogramowania i automatycznie przenosić zainfekowane obiekty do kwarantanny. Kwarantanna musi umożliwiać pobranie oryginalnego pliku lub jego bezpiecznej wersji (zabezpieczonej hasłem) przez administratora.

3. Zarządzanie Podatnościami i Aktualizacjami (Vulnerability & Patch Management) System musi posiadać zintegrowany moduł skanowania podatności, niewymagający instalacji dodatkowych agentów czy konsol. Skaner musi automatycznie, zgodnie z harmonogramem (nie rzadziej niż raz dziennie), weryfikować system operacyjny oraz zainstalowane aplikacje firm trzecich pod kątem znanych luk bezpieczeństwa. Baza podatności musi zawierać minimum **35 000 rekordów CVE**, a wyniki skanowania muszą prezentować punktację CVSS oraz ocenę ryzyka producenta. Moduł musi umożliwiać **automatyczne zarządzanie aktualizacjami (Patching)** dla minimum 150 popularnych aplikacji. Administrator musi posiadać możliwość tworzenia "białych list" (aplikacje aktualizowane automatycznie) oraz "czarnych list" (aplikacje wykluczone z automatycznej aktualizacji). Proces instalacji poprawek musi być inicjowany bezpośrednio z poziomu konsoli antywirusowej, z opcją ręcznego wymuszenia aktualizacji na wybranych stacjach.

VI. Moduł XDR (Extended Detection and Response) i Analityka Śledcza

W celu zapewnienia zaawansowanej detekcji i reagowania na incydenty, Zamawiający wymaga dostarczenia modułu klasy XDR, w pełni zintegrowanego z oprogramowaniem antywirusowym. Dostęp do konsoli centralnego zarządzania XDR musi odbywać się poprzez interfejs WWW zabezpieczony protokołem szyfrowanym SSL. Kluczowym wymogiem architektonicznym jest integracja danych: serwer administracyjny XDR musi przysyłać

Załącznik nr 1.8

zdarzenia i alerty bezpośrednio do głównej konsoli zarządzającej produktem antywirusowym tego samego producenta, zapewniając spójny widok bezpieczeństwa (Single Pane of Glass).

1. Reguły Detekcji i Zarządzanie Wyjątkami System musi zostać dostarczony z biblioteką **ponad 900 wbudowanych reguł bezpieczeństwa**, których naruszenie wyzwala alarm. Administrator musi posiadać pełną swobodę w tworzeniu własnych reguł oraz edycji reguł dostarczonych przez producenta. Rozwiązanie musi oferować zaawansowany mechanizm zarządzania wykluczeniami (False Positives):

- a. Możliwość wprowadzania wykluczeń dla konkretnego procesu lub procesu „rodzica”.
- b. Utworzenie wykluczenia musi skutkować automatycznym rozwiązaniem (zamknięciem) wszystkich aktywnych alarmów pasujących do definicji tego wykluczenia.
- c. Kryteria wykluczeń muszą być konfigurowalne w oparciu o szeroki zestaw atrybutów, w tym co najmniej: nazwę procesu, ścieżkę, wiersz polecenia (Command Line), wydawcę certyfikatu, typ podpisu, sumę kontrolną (SHA-1), nazwę komputera, grupę oraz użytkownika.

2. Analityka Procesów i Plików Wykonywalnych Administrator musi posiadać narzędzia do głębokiej weryfikacji plików uruchomionych na stacjach roboczych. System musi prezentować szczegółowe metadane każdego procesu, w tym: sumę kontrolną SHA-1, typ podpisu cyfrowego, wydawcę, opis i wersję pliku, nazwę i wersję produktu, oryginalną nazwę pliku, jego rozmiar oraz globalną reputację i popularność (w oparciu o dane z chmury producenta). W ramach zarządzania incydem, administrator musi mieć możliwość podjęcia natychmiastowych akcji wobec plików wykonywalnych (EXE) oraz bibliotek (DLL):

- a. Oznaczenia pliku jako bezpieczny.
- b. Pobrania pliku do analizy śledczej.
- c. Zablokowania pliku globalnie w organizacji.
- d. Blokada po sumie kontrolnej (Hash) musi umożliwiać dodanie komentarza oraz konfigurację akcji następczej (np. "Zabij proces i usuń plik").

3. Inspekcja Skryptów i Korelacja Zdarzeń Rozwiązanie musi zapewniać widoczność uruchamianych skryptów systemowych (np. PowerShell), prezentując parametry ich uruchomienia. Dla celów dowodowych, administrator musi mieć możliwość szczegółowego podglądu wykonanych czynności w formie tekstowej (co dokładnie skrypt próbował wykonać). System musi umożliwiać manualną ocenę skryptu (oznaczenie jako bezpieczny/niebezpieczny). W ramach analizy śledczej (Forensics), przy przeglądaniu szczegółów pliku wykonywalnego lub skryptu, system musi wizualizować powiązane zdarzenia w formie drzewa procesów lub listy, obejmującej co najmniej: modyfikacje plików i kluczy rejestru, zestawione połączenia sieciowe oraz utworzone pliki podrzędne.

4. Integracja Operacyjna i Reagowanie Konsola XDR musi wspierać efektywną pracę analityka poprzez możliwość tagowania obiektów oraz kontekstowe przełączanie się do konsoli antywirusowej. Z poziomu widoku szczegółów stacji w XDR, administrator musi mieć możliwość bezpośredniego przejścia do widoku tej samej stacji w konsoli AV, aby zweryfikować parametry sprzętowe (producent, model, nr seryjny, CPU, RAM, dyski) oraz listę zainstalowanego oprogramowania firm trzecich. Jako mechanizm aktywnego reagowania na incydent, konsola musi umożliwiać nawiązanie zdalnego połączenia ze stacją roboczą w celu wykonywania poleceń diagnostycznych i naprawczych (np. poprzez zdalny terminal PowerShell).

VII. System Uwierzytelniania Dwuskładnikowego (MFA) i Szyfrowanie

1. Szyfrowanie (Full Disk Encryption): System musi umożliwiać zarządzanie natywnym szyfrowaniem BitLocker (Windows) i FileVault (macOS) z poziomu konsoli antywirusowej, z obsługą uwierzytelniania Pre-Boot (TPM+PIN) i centralnym przechowywaniem kluczy odzyskiwania.

2. Uwierzytelnianie (MFA): W ramach przedmiotu zamówienia Wykonawca dostarczy i wdroży zintegrowany system silnego uwierzytelniania (2FA/MFA), mający na celu zabezpieczenie dostępu do firmowych zasobów, sieci oraz aplikacji. Rozwiązanie to musi charakteryzować się szeroką kompatybilnością środowiskową, zapewniając pełne wsparcie dla systemów operacyjnych **Microsoft Windows Server** (w wersjach: 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, aż do 2022, w tym edycje Essentials i SBS) oraz systemów stacji roboczych z rodziny **Windows** (od wersji 7, przez 8/8.1, 10, aż do 11), zarówno w architekturze 32-bitowej, jak i 64-bitowej.

Kluczowym wymaganiem jest zdolność rozwiązania do natywnej integracji z aplikacjami biznesowymi Microsoft. System musi zabezpieczać proces logowania do serwerów pocztowych **Microsoft Exchange** (wersje 2007/2010/2013/2016/2019), platformy **Microsoft SharePoint** (wersje 2010/2013/2016/2019) oraz systemu **Microsoft Dynamics CRM** (wersje 2011-2016). W zakresie ochrony dostępu zdalnego, rozwiązanie musi integrować się z usługami Microsoft Remote Desktop Web Access (RD Web), Terminal Services Web Access oraz Remote Web Access, wymuszając podanie drugiego składnika podczas logowania spoza sieci firmowej.

Dla zapewnienia uniwersalności ochrony, system musi posiadać wbudowany, własny **serwer RADIUS**. Musi on umożliwiać dodanie uwierzytelniania dwuskładnikowego do dowolnych rozwiązań VPN (Virtual Private Network) oraz urządzeń sieciowych wspierających protokół RADIUS, niezależnie od ich producenta.

Głównym narzędziem uwierzytelniającym ma być **aplikacja mobilna**, dostarczana przez producenta rozwiązania w ramach zakupionej licencji (bez dodatkowych opłat). Aplikacja ta musi spełniać następujące wymagania:

- 1. Kompatybilność:** Wsparcie dla urządzeń mobilnych z systemem Android (wersja 4.4 lub nowsza) oraz iOS (wersja 12 lub nowsza).
- 2. Bezpieczeństwo:** Możliwość dodatkowego zabezpieczenia dostępu do aplikacji za pomocą indywidualnego kodu PIN użytkownika.
- 3. Działanie Offline:** Generowanie haseł jednorazowych (OTP) musi odbywać się lokalnie na urządzeniu, bez konieczności posiadania aktywnego połączenia z Internetem w momencie logowania.
- 4. Wielodostęp:** Możliwość obsługi wielu kont (tokenów) dla różnych serwerów uwierzytelniających w ramach jednej instalacji aplikacji.

Alternatywnie do aplikacji mobilnej, system musi umożliwiać dostarczanie haseł jednorazowych za pomocą wiadomości **SMS**. Wsparcie techniczne dla całego modułu MFA musi być świadczone w języku polskim przez autoryzowanego dystrybutora producenta.

VIII. Usługa Wdrożenia i Migracji (Specyfikacja Techniczna)

W ramach ceny oferty, Wykonawca zobowiązany jest do przeprowadzenia kompleksowej usługi wdrożeniowej w formie zdalnej asysty technicznej. Zakres prac jest uzależniony od zaoferowanego rozwiązania:

Załącznik nr 1.8

Scenariusz A: W przypadku kontynuacji rozwiązania posiadanego (Upgrade):

Wykonawca przeprowadzi migrację środowiska zarządzającego z obecnej konsoli lokalnej (On-Prem) do nowej instancji chmurowej. Proces ten musi odbyć się z wykorzystaniem narzędzi migracyjnych producenta, bez konieczności ręcznej reinstalacji agentów na stacjach końcowych. Następnie Wykonawca dokona aktywacji i konfiguracji nowych modułów (XDR, Szyfrowanie, MFA, Podatności), w tym przeprowadzi tuning reguł detekcji przez okres minimum 7 dni oraz audyt obecnych polityk bezpieczeństwa.

Scenariusz B: W przypadku zaoferowania rozwiązania równoważnego (Inny Producent): Wykonawca zobowiązany jest do przeprowadzenia pełnego procesu wymiany oprogramowania, zgodnie z wymaganiami opisanymi w Rozdziale X (Wymagania dla rozwiązań równoważnych).

W obu przypadkach wdrożenie kończy się dostarczeniem dokumentacji powykonawczej oraz szkoleniem dla administratorów Zamawiającego.

IX. Wsparcie Producenta rozwiązania

Wsparcia Producenta – zapewniającego ciągłość działania oprogramowania i dostęp do aktualizacji.

Wsparcie Producenta (Gwarancja Technologiczna) Wykonawca dostarczy licencje z aktywnym pakietem Maintenance producenta, który gwarantuje Zamawiającemu:

- Prawo do pobierania i instalacji najnowszych wersji oprogramowania (Upgrade) oraz poprawek (Patches/Hotfix) wydawanych przez producenta.
- Ciągłą, automatyczną aktualizację baz sygnatur wirusów, modułów skanujących oraz reguł detekcji behawioralnej.
- Gwarancję dostępności konsoli chmurowej na poziomie określonym w SLA producenta (nie niższym niż 99,5%).
- Dostęp do globalnej bazy wiedzy (Knowledge Base) oraz wsparcia III linii (Vendor Support) w przypadku błędów krytycznych w kodzie oprogramowania.

X. Wymagania dotyczące rozwiązań równoważnych (Klauzula Migracyjna)

Zamawiający informuje, że w obecnej infrastrukturze wykorzystuje oprogramowanie ESET PROTECT Essential On-Prem. Dopuszcza się składanie ofert na rozwiązania równoważne innych producentów, pod warunkiem spełnienia wszystkich wymogów funkcjonalnych OPZ.

Ze względu na charakter zamówienia (rozbudowa i przedłużenie ochrony), w przypadku zaoferowania oprogramowania innego niż obecnie posiadane, Wykonawca w ramach ceny oferty zobowiązany jest do przeprowadzenia **pełnej migracji środowiska**. Proces ten musi obejmować:

1. Skuteczną i bezpieczną deinstalację dotychczasowych agentów ze wszystkich stacji roboczych i serwerów.
2. Instalację i konfigurację nowego oprogramowania.
3. Ręczne odtworzenie wszystkich polityk bezpieczeństwa, reguł firewalla, wykluczeń i struktury grup w nowym systemie.
4. Zapewnienie ciągłości ochrony antywirusowej podczas procesu migracji.

Załącznik nr 1.8

5. Przeprowadzenie rozszerzonego, trzydniowego szkolenia dla administratorów, wyrównującego ich poziom wiedzy z obsługi nowego systemu do poziomu systemu dotychczasowego.

Wszelkie koszty techniczne i osobowe związane z procesem migracji na rozwiązanie innego producenta ponosi Wykonawca.