

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup (przedłużenie) licencji na oprogramowanie antywirusowe na okres 12 miesięcy.

I. Przedmiot zamówienia

- 1 Przedmiotem zamówienia jest dostarczenie (przedłużenie) dwóch 12-miesięcznych subskrypcji na oprogramowanie **ESET PROTECT Entry** (identyfikator licencji 3AM-C3J-KFM) **w ilości 2500 sztuk** oraz **ESET PROTECT Elite** (identyfikator licencji 3B3-76F-8HX) **w ilości 120 sztuk**.
- 2 Okres ważności zakupionych licencji:
 - a. ESET PROTECT Entry: od dnia **08.05.2026 r.** na okres 12 miesięcy
 - b. ESET PROTECT Elite: od dnia **13.07.2026 r.** na okres 12 miesięcy
- 3 Termin dostawy zamówienia: 5 dni roboczych od dnia podpisania umowy.
- 4 Zamawiający posiada obecnie licencję na oprogramowanie ESET PROTECT Entry dla 2500 urządzeń, które obowiązują do dnia 08.05.2026 r. oraz ESET PROTECT Elite dla 120 urządzeń, które obowiązują do dnia 13.07.2026 r.
- 5 Oprogramowanie i licencje muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
- 6 Zamawiający wymaga poświadczenia na dostępnym dla Zamawiającego portalu licencyjnym producenta lub dostarczenia wraz z licencjami certyfikatu lub oświadczenia przedstawiciela producenta potwierdzającego ważność i zakres uprawnień licencyjnych oraz datę wystawienia oświadczenia.
- 7 Zamawiający dopuszcza rozwiązanie równoważne pod warunkiem spełnienia wszystkich poniższych funkcjonalności.

II. Rozwiązanie równoważne dla ESET PROTECT Entry:

Konsola Zarządzająca

- 1 Rozwiązanie musi posiadać możliwość zarządzania z konsoli w wersji lokalnej (on-premise) oraz chmurowej (SaaS) hostowanej przez producenta, przynajmniej w języku polskim i angielskim.
- 2 Rozwiązanie musi wykorzystywać dedykowanego agenta, który pośredniczy w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania a także pomiędzy zarządzanym urządzeniem a serwerami aktualizacji producenta.
- 3 Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

- 4 Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - a. Google Authenticator,
 - b. Microsoft Authenticator,
 - c. Authy,
 - d. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
- 5 Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
 - a. Wyrażenie CRON,
 - b. Codziennie,
 - c. Cotygodniowo,
 - d. Co miesiąc,
 - e. Co rok,
 - f. Po wystąpieniu nowego zdarzenia,
 - g. Po automatycznym umieszczeniu hosta w grupie dynamicznej lub analogicznym rozwiązaniu.
- 6 Rozwiązanie musi udostępniać minimum 80 szablonów raportów przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
- 7 Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej protokołu Syslog.
- 8 Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
 - a. JSON.
 - b. LEEF.
 - c. CEF.

Ochrona Punktów Końcowych (Windows, macOS, Linux)

Konsola Zarządzająca

- 1 Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- 2 Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
- 3 Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
 - a. Ubuntu Desktop 22.04 LTS,
 - b. Ubuntu Desktop 24.04 LTS,
 - c. Red Hat Enterprise Linux 8, 9, 10,

- d. Linux Mint 21, 22.
- 4 Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu:
- a. Wirus.
 - b. Trojan.
 - c. Robak.
 - d. Adware.
 - e. Spyware.
 - f. Dialer.
 - g. Phishing.
 - h. Backdoor.
- 5 Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 6 Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
- 7 Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
- 8 Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 9 Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- 10 Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
- a. Całego dysku.
 - b. Wybranych katalogów.
 - c. Pojedynczych plików.
 - d. Plików spakowanych oraz skompresowanych.
 - e. Dysków sieciowych.
 - f. Dysków przenośnych.
- 11 Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
- a. Wybranych plików.
 - b. Wybranych procesów.
 - c. Wybranych lokalizacji.

- d. Wybranych rozszerzeń.
 - e. Nazwy wykrycia.
 - f. Sumy kontrolnej (SHA1).
- 12 Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
- 13 Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
- a. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - b. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - c. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
 - d. Wszelkie dane przesyłane w ramach systemu wczesnego ostrzegania oraz analizy chmurowej muszą być przetwarzane i składowane na serwerach zlokalizowanych w obrębie Europejskiego Obszaru Gospodarczego (EOG).
- 14 Rozwiązanie musi udostępniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- 15 Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
- 16 Rozwiązanie musi udostępniać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 17 Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
- a. Typ urządzenia:
 - Pamięci masowe.
 - Optyczne pamięci masowe.
 - Pamięci masowe Firewire.
 - Urządzenia do tworzenia obrazów.
 - Drukarki USB.
 - Urządzenia Bluetooth.
 - Czytniki kart inteligentnych.
 - Modemy.

- Porty LPT/COM.
 - Urządzenia przenośne.
- b. parametry urządzenia:
- Numer seryjny.
 - Producent.
 - Model.
- c. typ dostępu:
- Brak możliwości zapisu.
 - Pełen dostęp.
 - Ostrzeżenie użytkownika.
 - Brak dostępu.
- 18 Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
- a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- 19 Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji. A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- 20 Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
- a. Raport musi posiadać co najmniej:
- Listę zainstalowanych aplikacji.
 - Listę usług systemowych.
 - Informacje o systemie operacyjnym i sprzęcie.
 - Listę aktywnych procesów i połączeń sieciowych.

- Harmonogram systemu operacyjnego.
 - Szczegóły pliku hosts.
 - Informacje o sterownikach.
- 21 Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
- a. Antywirus.
 - b. Zapora osobista.
 - c. Sandbox.
 - d. Antyspyware.
 - e. Metody heurystyczne.
- 22 Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
- 23 Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- a. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
 - b. Ochrona musi być realizowana w oparciu o co najmniej:
 - globalna czarna lista RBL,
 - czarna lista użytkownika,
 - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- 24 Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- a. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - Skanowanie portów TCP oraz UDP,
 - Wykrywanie duplikacji adresu IP,
 - Atak zatruwania ARP,
 - Nieprawidłowa długość pakietu TCP oraz UDP.
 - b. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - RDP,
 - SMB,
 - My SQL,

- MS SQL.
 - c. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
- 25 Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
- a. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
 - b. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
- 26 Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
- a. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
 - b. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
 - c. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
- 27 Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
- a. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
 - b. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
 - Treść komunikatu.
 - Obraz.

Ochrona Serwerów i Środowisk Wirtualnych

- 1 Wsparcie Systemów: Pełna obsługa Windows Server (od 2012 R2 do 2025) oraz Linux (RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux)
- 2 Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
 - a. MS SQL.
 - b. Active Directory.
 - c. IIS.
 - d. Sysvol.
 - e. DNS.
 - f. DHCP.
 - g. Hyper-V.
 - h. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
- 3 Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - a. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - Skanowanie portów TCP oraz UDP,
 - Wykrywanie duplikacji adresu IP,
 - Atak zatrutowania ARP,
 - Nieprawidłowa długość pakietu TCP oraz UDP.
 - b. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - RDP,
 - SMB,
 - My SQL,
 - MS SQL.
 - c. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
- 2 Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
- 3 Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

- 4 Zapora osobista musi posiadać co najmniej cztery tryby pracy:
- 5 tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - a. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - b. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - c. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Zarządzanie Urządzeniami Mobilnymi (MDM/MTD) w chmurze

- 1 MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
- 2 MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - a. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - b. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - c. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - d. Apple Business Manager (ABM),
 - e. Android Enterprise (co najmniej w zakresie Device Owner).
- 3 MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - a. usunięcie zawartości urządzenia,
 - b. przywrócenie urządzenia do ustawień fabrycznych,
 - c. zablokowanie urządzenia,
 - d. uruchomienie sygnału dźwiękowego,
 - e. lokalizację GPS,
 - f. Resetowanie hasła blokady ekranu.
- 4 MDM musi zapewniać administratorowi podejrzanie listy zainstalowanych aplikacji.
- 5 MDM musi umożliwiać co najmniej:
 - a. Dla systemów iOS oraz iPadOS
 - konfigurację kont e-mail,
 - konfigurację połączeń VPN,
 - Konfigurację połączeń Wi-Fi,

- Konfigurację listy certyfikatów,
- możliwość uruchomienia trybu jednej aplikacji.

b. Dla systemu Android:

- blokadę wykonywania połączeń,
- blokadę konfiguracji sieci Wi-Fi,
- blokadę konfiguracji tuneli VPN,
- zarządzanie aktualizacjami systemu operacyjnego,
- blokadę zmiany tapety urządzenia.

Wsparcie i Język

- 1 Serwis: Pełne wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera w języku polskim przez cały okres licencjonowania.

III. Rozwiązanie równoważne dla ESET PROTECT Elite:

Konsola Zarządzająca

Funkcjonalność Taka jak w przypadku rozwiązania równoważnego dla ESET PROTECT Entry

Ochrona Punktów Końcowych (Windows, macOS, Linux)

Funkcjonalność Taka jak w przypadku rozwiązania równoważnego dla ESET PROTECT Entry

Ochrona Serwerów i Środowisk Wirtualnych

Funkcjonalność Taka jak w przypadku rozwiązania równoważnego dla ESET PROTECT Entry

Zarządzanie Urządzeniami Mobilnymi (MDM/MTD)

Funkcjonalność Taka jak w przypadku rozwiązania równoważnego dla ESET PROTECT Entry

Sandbox w chmurze

- 1 Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
- 2 Wszelkie dane przesyłane w ramach tej funkcjonalności muszą być przetwarzane i składowane na serwerach zlokalizowanych w obrębie Europejskiego Obszaru Gospodarczego (EOG).
- 3 Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- 4 Rozwiązanie musi wspierać systemy w tym co najmniej:
 - a. Microsoft Windows 10 oraz 11,
 - b. Microsoft Windows Server,

- c. macOS 11 (Big Sur) oraz nowszych
 - d. RedHat Enterprise Linux (RHEL),
 - e. Rocky Linux,
 - f. Ubuntu,
 - g. Debian,
 - h. SUSE Linux Enterprise Server (SLES),
 - i. Oracle Linux,
 - j. Amazon Linux.
- 5 Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 6 Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
- 7 Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
- a. archiwa,
 - b. skrypty,
 - c. pliki wykonywalne,
 - d. pliki rejestru systemowego (.reg),
 - e. możliwy spam,
 - f. dokumenty.
- 8 Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
- a. natychmiast po ich przeanalizowaniu,
 - b. po upływie 30 dni,
 - c. nigdy.
- 9 Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 10 9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 11 Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
- 12 Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

- 13 Rozwiązanie pozwala na wystanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
- a. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
- 14 Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
- a. czysty,
 - b. podejrzany,
 - c. bardzo podejrzany,
 - d. szkodliwy.
- 15 W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
- A. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
 - a. przeglądarki internetowej,
 - b. programy poczty e-mail,
 - c. nośniki wymienne,
 - d. pliki wyodrębnione z archiwum.
- 16 Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

Szyfrowanie

- 1 Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- 2 Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
- 3 Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- 4 Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
- 5 Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
 - a. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
 - b. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
 - c. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
 - d. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.

- e. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
 - f. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
- 6 Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
 - 7 Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
 - 8 Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
 - 9 Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.
 - 10 W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.
 - 11 Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia w przypadku aktualizacji systemu operacyjnego.

Endpoint Detection and Response / eXtended Detection and Response

- 1 Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- 2 Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- 3 Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
 - a. Tworzenie procesów.
 - b. Uruchamianie, zatrzymanie i modyfikacja usług.
 - c. Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym.
 - d. Usuwanie oraz zmiana nazw plików.
 - e. Tworzenie i usuwanie kluczy rejestru systemowego.
 - f. Ładowanie bibliotek DLL.
 - g. Zalogowanie użytkowników. A. elementy sieciowe, w tym co najmniej:
 - h. Pobranie plików wykonywalnych.
 - i. Zestawienie połączeń TCP/IP.
 - j. Zapytania http.
 - k. Zapytania DNS.
- 4 Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

- a. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
 - Blokowanie pliku wykonywalnego.
 - Blokowanie pliku wykonywalnego i poddanie go kwarantannie.
 - Blokowanie podejrzanej biblioteki DLL.
 - Zakończenie procesu.
 - Skanowanie komputera w poszukiwaniu zagrożeń.
 - Wyłączenie komputera.
 - Izolacja sieciowa hosta dla systemów Windows oraz Linux.
 - Wylogowanie użytkownika.
 - b. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.
- 5 Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
- a. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
 - b. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:
 - Proces.
 - Proces nadrzędny (proces rodzica).
 - Nazwę procesu.
 - Ścieżkę procesu.
 - Wiersz polecenia.
 - Wydawcę.
 - Typ podpisu cyfrowego.
 - SHA-1.
 - SHA-2.
 - Użytkownika.
 - c. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
- 6 Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.

- a. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
 - b. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):
 - SHA-1.
 - SHA-256.
- 7 Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
- 8 Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
 - a. Oznaczania ich jako bezpieczne lub niebezpieczne.
 - b. Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - c. Zablokowania wykonywania i wykorzystania pliku.
 - d. Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
- 9 Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
 - a. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
 - b. Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - c. Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
 - d. Administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
 - e. Administrator musi posiadać możliwość odczytania informacji o języku skryptu.
- 10 Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
 - a. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
- 11 Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
- 12 Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.
- 13 Rozwiązanie musi umożliwiać moduł zaawansowanego wyszukiwania, które umożliwia badanie wskaźników danych zawartych w XDR, przynajmniej w oparciu o:
 - a. Wyszukiwanie dowolnego tekstu.

- b. Wyszukiwanie, pozwalające łączyć ze sobą różne słowa, oddalone od siebie nie więcej niż 3 innymi słowami.
- c. Wyszukiwanie po nazwie procesów.
- d. Wyszukiwanie po ocenie ryzyka.
- e. Filtrowanie według daty.

Ochrona serwerów w chmurze AWS, Microsoft Azure i Google Cloud Platform

- 1 Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
- 2 Rozwiązanie musi udostępniać możliwość integracji przynajmniej z rozwiązaniami:
 - a. Microsoft Azure.
 - b. Google Cloud Platform.
 - c. Amazon Web Services.
- 3 Rozwiązanie powinno zapewniać możliwość zarówno automatycznego uruchamiania ochrony dla nowych i już istniejących maszyn wirtualnych, jak i ręcznego wskazania wybranych zasobów do objęcia ochroną.

Wsparcie techniczne

Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.