

Załącznik nr 3 do zapytania ofertowego

Popielów, 03.10.2024 r.

## Opis przedmiotu zamówienia

Przedmiot zamówienia obejmuje dostarczenie przez Wykonawcę 60 licencji oprogramowania antywirusowego w wersji **ESET Elite** lub „równoważnej” na 2 lata wraz z konsolą zarządzającą dla Urzędu Gminy w Popielowie oraz przeprowadzenie certyfikowanego szkolenia dla administratora Zamawiającego w zakresie konfiguracji i zarządzania narzędziem Extended Detection & Response (XDR) lub „równoważnym” w języku polskim przez autoryzowanym centrum szkoleniowym, zakończone certyfikatem lub zaświadczeniem ukończenia szkolenia.

### I. Wymagania dot. szkolenia:

1. Szkolenie należy przeprowadzić do 31.12.2024 r.
2. Szkolenie może być przeprowadzone w wersji online lub stacjonarnie w siedzibie Zamawiającego
3. Czas szkolenia minimum 6 godzin,
4. Szkolenie i udostępnione materiały szkoleniowe muszą być w języku polskim.
5. Po szkoleniu uczestnik powinien zdobyć wiedzę i umiejętność obsługi narzędzia XDR a także: wykryć zagrożenia APT, wykrywać unikatowe pliki w sieci, monitorować aplikację, wykonywać analizę powłamaniovą, chronić firmę przed ransomware, blokować uruchamianie pliku w sieci.

### II. Wymagania dot. oferowanej licencji oprogramowania antywirusowego:

1. Zamawiający posiada obecnie licencję źródłową **33C-6FT-RNX, ESET PROTECT Entry ON-PREM**, ważną do dnia: **2024-10-17**

Wykonawca powinien dostarczyć licencję do dnia 16.10.2024 r. w celu zapewnienia ciągłości zabezpieczenia antywirusowego.

#### 2. Minimalne wymagania dla oprogramowania antywirusowego:

Oprogramowanie antywirusowe bez względu na wybór przez Wykonawcę producenta oprogramowania musi spełniać następujące wymagania Zamawiającego:

- 1) Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
- 2) Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
- 3) Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
- 4) Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- 5) Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- 6) Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- 7) Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
- 8) Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

- 9) Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
- 10) Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- 11) Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
- 12) Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, co tygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
- 13) Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- 14) Rozwiązanie musi wspierać architekturę ARM64.
- 15) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- 16) Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
- 17) Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- 18) Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- 19) Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- 20) Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
- 21) Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
- 22) Rozwiązanie musi integrować się z Intel Threat Detection Technology.
- 23) Rozwiązanie musi zapewniać 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).
- 24) Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
- 25) Rozwiązanie musi posiadać 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 heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 26) Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

- 27) Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
- 28) Moduł HIPS 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.
- 29) Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
- 30) 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.
- 31) Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- 32) Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
- 33) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- 34) Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
- 35) Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
  - a) tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
  - b) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  - c) tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
  - d) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
- 36) Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
- 37) Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

- 38) Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- 39) Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
- 40) Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
- 41) Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 42) W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
- 43) Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 8.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
- 44) Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- 45) Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- 46) Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
- 47) Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- 48) Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- 49) Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- 50) Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
- 51) Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- 52) Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
- 53) Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
- 54) Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- 55) Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- 56) Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

- 57) Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
- 58) Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- 59) Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
- 60) Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- 61) Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- 62) Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
- 63) Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
- 64) System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
- 65) System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
- 66) Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
- 67) Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- 68) Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
- 69) Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
- 70) Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- 71) Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
- 72) Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
  - a) usunięcie zawartości urządzenia,
  - b) przywrócenie urządzenia do ustawień fabrycznych,
  - c) zablokowania urządzenia,
  - d) uruchomienie sygnału dźwiękowego,
  - e) lokalizację GPS.
- 73) Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- 74) Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
  - a) nazwę aplikacji,
  - b) nazwę pakietu,
  - c) kategorię sklepu Google Play,
  - d) uprawnienia aplikacji,
  - e) pochodzenie aplikacji z nieznanego źródła.

- 75) Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
- 76) Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
- 77) Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
- 78) Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
- 79) Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
- 80) Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
- 81) Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
- 82) System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
- 83) Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
- 84) Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
- 85) Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 86) Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- 87) Rozwiązanie musi wykorzystywać do działania chmurę producenta.
- 88) Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- 89) Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- 90) Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- 91) Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- 92) Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
- 93) Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
- 94) Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- 95) Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
- 96) Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
- 97) Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:



- a) Czysty,
  - b) Podejrzany,
  - c) Bardzo podejrzany,
  - d) Szkodliwy.
- 98) W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
- 99) W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
- 100) Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
- 101) Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
- 102) Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365.
- 103) Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
- 104) Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
- 105) Rozwiązanie musi być dostępny w języku polskim.
- 106) Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
- 107) użytkowników, otrzymujących najwięcej spamu,
- 108) użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
- 109) użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
- 110) kont użytkowników, które mogą być podejrzane.
- 111) Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
- 112) Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
- a) jaka ilość wiadomości została przeskanowana,
  - b) wynik skanowania poszczególnej wiadomości,
  - c) czynność podjęta przez rozwiązanie.
- 113) Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
- a) zagrożeniach, które zostały wykryte,
  - b) na jakim koncie zostały wykryte,
  - c) jakie zagrożenie zostało wykryte,
  - d) podjętą czynność.
- 114) Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
- 115) Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
- 116) Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
- 117) Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
- a) wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
  - b) wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,

- c) dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
- 118) Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
  - 119) Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
  - 120) Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
  - 121) Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
  - 122) Rozwiązanie musi posiadać możliwość przysyłania powiadomień e-mail z funkcją wyboru preferowanego języka.
  - 123) Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
  - 124) Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
  - 125) Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
  - 126) Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
  - 127) Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
  - 128) Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
  - 129) Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
  - 130) Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
  - 131) Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
  - 132) Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
  - 133) Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
  - 134) Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
  - 135) W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
  - 136) W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.



- 137) Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
- 138) Konsola administracyjna musi mieć możliwość tagowania obiektów.
- 139) Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
- 140) Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
- 141) Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
- 142) Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
- 143) Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
- 144) Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
- 145) Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
- 146) Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
- 147) Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
- 148) Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
- 149) Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
- 150) Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
- 151) Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
- 152) Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.

- 153) Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.
- 154) Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
- 155) Rozwiązanie musi wspierać system operacyjny Windows 10 / Windows 11.
- 156) Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
- 157) Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
- 158) Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
- 159) Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
- 160) Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
- 161) Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
- 162) Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
- 163) Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
- 164) Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
- 165) Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
- 166) Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
- 167) Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
- 168) Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
- 169) Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
- 170) Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.

### III. Rozwiązania równoważne:

Wykonawca może zaproponować i dostarczać 60 licencji oprogramowania antywirusowego innego producenta (równoważnego) niż firmy Eset w wersji ESET Elite. W przypadku zaproponowania rozwiązania równoważnego licencji oprogramowania muszą być wspierane przez producenta oprogramowania do dnia 17.10.2026 r. oraz spełniać minimalne wymagania opisane powyżej.

W przypadku zaoferowania przeprowadzenia szkolenia w zakresie konfiguracji i zarządzania narzędziem „równoważnym” do Extended Detection & Response (XDR) modułu ESET Protect Elite, szkolenie musi dotyczyć obsługi, zarządzania i konfiguracji całego systemu antywirusowego.

1. W przypadku, gdy w zapytaniu ofertowym i jego załącznikach zostały użyte znaki towarowe, patenty, pochodzenia/źródła lub szczególne procesy oznacza to, że są podane przykładowo jako kontynuację obecnie posiadanego sprzętu i oprogramowania oraz określają jedynie minimalne oczekiwane parametry jakościowe, techniczne, wydajnościowe oraz wymagany standard, a każdemu odniesieniu użytemu w powyższej dokumentacji towarzyszy **wyraz „lub równoważne”**. Ewentualne podane w opisach nazwy własne, znaki towarowe, patenty, pochodzenia/źródła lub szczególne procesy, nie mają na celu naruszenia przepisów prawa, a mają jedynie za zadanie sprecyzowanie oczekiwań dot. parametrów technicznych, jakościowych, technologicznych i wydajnościowych oraz zachowania kompatybilności z obecnie posiadanym sprzętem i oprogramowaniem. Wykonawca może zastosować materiały lub produkty lub urządzenia lub procesy równoważne, lecz o parametrach technicznych, jakościowych, funkcjonalnych, wydajnościowych, użytkowych i technologicznych podobnych lub lepszych - nie gorszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie i użytkowanie już posiadanych rozwiązań przyjętych przez Gminę Popielów w posiadanym sprzęcie i oprogramowaniu; Równoważne rozwiązania muszą być dopuszczone do obrotu i stosowania zgodnie z obowiązującym prawem;
  - 1) Wykonawca, który na etapie składania ofert ma zamiar zaoferować urządzenia lub produkty lub materiały lub procesy równoważne, zobowiązany jest wykazać wraz z ofertą (**przez złożenie stosownych dokumentów**, oświadczeń, itp.), że zastosowane przez niego urządzenia, produkty, materiały lub procesy spełniają wymagania określone przez Zamawiającego;
  - 2) Obowiązek Wykonawcy wykazania równoważności może być spełniony w jakiegokolwiek sposób pozwalający Zamawiającemu **jednoznacznie** stwierdzić zgodność oferowanych w ofercie urządzeń, produktów, materiałów lub procesów z wymaganiami określonymi w zapytaniu ofertowym i jego załącznikach;
  - 3) Zamawiający oceni spełnienie powyższych wymogów w zakresie równoważności proponowanych urządzeń, produktów, materiałów lub procesów poprzez sprawdzenie złożonych przez Wykonawcę dokumentów, oświadczeń, itp. Zamawiający oceni (porówna) czy parametry techniczne, jakościowe, funkcjonalne, wydajnościowe, użytkowe i/lub technologiczne są podobne lub lepsze – nie gorsze, niż wymagane w zapytaniu ofertowym i jego załącznikach, zgodnie z powyższymi zapisami;
  - 4) W przypadku nie dołączenia dokumentów, oświadczeń, itp. uwiarygadniających zastosowanie urządzeń, produktów, materiałów lub procesów równoważnych Zamawiający wezwie oferenta do ich uzupełnienia;
  - 5) W przypadku gdy zaoferowane rozwiązanie równoważne nie będzie spełniać przynajmniej minimalnych wymagań opisanych powyżej Zamawiający odrzuci taką ofertę jako nie odpowiadającą treści zapytania ofertowego;
2. Użycie w zapytaniu ofertowym i jego załącznikach etykiety oznacza, że Zamawiający akceptuje wszystkie etykiety potwierdzające, że dane dostawy lub usługi spełniają **równoważne** wymagania określonej przez Zamawiającego etykiety. W przypadku gdy Wykonawca z przyczyn od niego niezależnych nie może uzyskać określonej przez Zamawiającego etykiety lub równoważnej etykiety, Zamawiający, w terminie, przez siebie wyznaczonym akceptuje inne odpowiednie środki dowodowe, w szczególności dokumentację techniczną producenta, o ile dany Wykonawca udowodni, że dostawy lub usługi, które mają zostać przez niego wykonane/dostarczone,

spełniają wymagania określonej etykiety lub określone wymagania wskazane przez Zamawiającego.

3. Użycie w dokumentacji opisującej przedmiot zamówienia wymogu posiadania certyfikatu wydanego przez jednostkę oceniającą zgodność lub sprawozdania z badań przeprowadzonych przez tę jednostkę jako środka dowodowego potwierdzającego zgodność z wymaganiami lub cechami określonymi w opisie przedmiotu zamówienia, kryteriach oceny ofert lub warunkach realizacji zamówienia oznacza, że zamawiający akceptuje również certyfikaty wydane przez inne równoważne jednostki oceniające zgodność. Zamawiający akceptuje także inne odpowiednie środki dowodowe, w szczególności dokumentację techniczną producenta, w przypadku, gdy dany Wykonawca nie ma ani dostępu do certyfikatów lub sprawozdań z badań, ani możliwości ich uzyskania w odpowiednim terminie, o ile ten brak dostępu nie może być przypisany danemu Wykonawcy, oraz pod warunkiem że dany Wykonawca udowodni, że wykonywane przez niego dostawy lub usługi spełniają wymogi lub kryteria określone w opisie przedmiotu zamówienia, kryteriach oceny ofert lub wymagania związane z realizacją zamówienia.
4. Zastosowane przez Wykonawcę materiały, produkty, wyroby lub rozwiązania równoważne muszą być co najmniej:
  - 1) tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
  - 2) o parametrach technicznych opisanych w zapytaniu ofertowym wraz z załącznikami (wzorzec jakościowy),
  - 3) spełniać te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp, ppoż,
  - 4) posiadać stosowne dokumenty (atesty, certyfikaty);