Załącznik nr 1 do SWZ

Przedmiot zamówienia został podzielony na dwie części:

Część pierwsza obejmuje dostawę kompleksowego rozwiązania technicznego, składającego się z następujących komponentów:

I. Zarządzalnych urządzeń sieciowych:
   a) 1 szt. przełącznika sieciowego typ I
   b) 2 szt. przełączników sieciowych typ II
   c) 3 szt. Access Point;

II. Serwerowego systemu operacyjnego i oprogramowania bezpieczeństwa: Systemu operacyjnego w ilości 2 szt.

III. Oprogramowania klasy XDR.

Część druga obejmuje usługę wsparcia.

Szczegółowy opis:

Część pierwsza:

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

1. Instalacja oraz konfiguracji oprogramowania zgodnie z wytycznymi Zamawiającego
2. Dostarczenie dokumentacji zawierającej specyfikację techniczną wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów.

Wymagania w zakresie instalacji i konfiguracji:

1. Montaż urządzeń w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Podłączenie urządzeń do listew zasilających PDU.
3. Aktualizacja oprogramowania układowego wszystkich komponentów.
4. Podłączenie do sieci LAN (rekonfiguracja dostarczanych przełączników)

Wszelkie opisane w niniejszym OPZ działania wykonawcy dotyczą rozwiązań dostarczanych w ramach niniejszego postępowania. W wypadku wystąpienia konieczności podjęcia jakichkolwiek działań w infrastrukturze Zamawiającego, celem realizacji przedmiotu niniejszego zamówienia, Zamawiający zobowiązuje się wykonać te działania we własnym zakresie.

UWAGA

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu ani do zmiany ceny.

I. Zarządzalne urządzenia sieciowe:

a) 1 szt. przełącznika sieciowego typ I

Zamawiający oczekuje dostawy 1 przełącznika sieciowego, spełniającego poniższe, minimalne wymagania:

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	Przełącznik sieciowy
Porty	Przełącznik musi posiadać: 24 x 10/100/1000BaseT 4 x 1G/10G/25G/50G1 SFP 1 x RJ45 do zarządzania
Obudowa	1U, umożliwiająca montaż w szafie rack 19 cali
Zdolność przełączania	Min. 440 Gbps
Przekazywanie (pakiet 64-bajtowy)	Min. 330 Mpps

Bezpieczeństwo	SSH
Rozmiar tablicy MAC	32K
Bufor pamięci	8MB
Procesor	Switch musi posiadać czterordzeniowy procesor o taktowaniu min. 1800MHz ARM,
Pamięć Ram	Switch musi posiadać pamięć RAM min. 8 GB
Pamięć Flash	Switch musi posiadać pamięć Flash min. 32 GB
Standardy	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3ad IEEE 802.3z
Inne	Przełączniki sieciowe muszą mieć możliwość połączenia w jedną spójną logiczną całość (stos).
Gwarancja	Min. 5 lat gwarancji producenta

b) 2 szt. przełącznika sieciowego typ II

Zamawiający oczekuje dostawy 2 przełączników sieciowych, spełniających poniższe, minimalne wymagania:

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	Przełącznik sieciowy
Porty	Przełącznik musi posiadać: 24 x 1GbE 4 x 1G SFP
Obudowa	1U, umożliwiająca montaż w szafie rack 19 cali
Zdolność przełączania	Min. 56 Gbps
Przekazywanie (pakiet 64-bajtowy)	Min. 41.6 Mpps
Bezpieczeństwo	SSH

Rozmiar tablicy MAC	8K
Bufor pamięci	4MB
Pamięć Ram	Switch musi posiadać pamięć RAM min. 256 MB
Pamięć Flash	Switch musi posiadać pamięć Flash min. 64 MB
Standardy	IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad LACP, IEEE 802.3z Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w RSTP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at
Gwarancja	Min. 3 lata gwarancji producenta

c) 3 szt. Access Point;

Zamawiający oczekuje dostawy 3 szt. Access Point, spełniającego poniższe, minimalne wymagania:

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	Access point
Częstotliwość	2,4 GHz 5 GHz
Maksymalna szybkość przesyłania danych	1770 Mbit/s

Maksymalna szybkość przesyłania danych (2.4 GHz)	570 Mbit/s
Maksymalna szybkość przesyłania danych (5 GHz)	1200 Mbit/s
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Standardy komunikacyjne	IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az
Automatyczne MDI/MDI-X	Tak
MIMO	Tak
Typ MIMO	Multi User MIMO
Metoda rozszerzenia obrazu	DSSS, OFDM, OFDMA
Modulacja	16-QAM, 64-QAM, 256-QAM, 1024-QAM, BPSK, CCK, QPSK
Szyfrowanie / bezpieczeństwo	WPA3, WPA, WPA2 Do przełącznika należy dostarczyć 4 szt. wkładek 10G MMF SR
Porty i interfejsy	Ethernet LAN (RJ-45) 1szt; USB 2.0 (USB typa A) 1szt.
Obsługa PoE	Tak
Maksymalne zużycie mocy	16,5 W
Zakres wilgotności względnej	5 - 93%
Zakres temperatur (eksploatacja)	0 - 50 °C
Zakres temperatur (przechowywanie)	-40 - 70 °C
Dopuszczalna wilgotność względna	5 - 93%
Inne wymagane	Zestaw montażowy, Zasilacz PoE.

II. Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa: System operacyjny - 2 szt.

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2025 Standard i wymagana dostarczenia dwóch licencji na oprogramowanie Microsoft Windows Server 2025 Standard 64-bit PL lub nowszy + do każdej z licencji dodatkowo 80 licencji CAL User lub równoważny serwerowy system operacyjny wraz z licencjami CAL User.

Opis równoważności oprogramowania

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wszystkie elementy systemu oraz jego licencja pochodzą od tego samego producenta.
2. Wymaga się dostarczenia odpowiedniej liczby licencji dla serwerów, 2 i 1- procesorowych, posiadających min 12 rdzeni,
3. Jeżeli wymagane jest posiadanie licencji dostępowych, należy dostarczyć licencję dla odpowiedniej liczby użytkowników.
4. Licencja na SSO zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 2 w środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji.
5. SSO posiada graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.
6. Obsługa do 48 TB RAM
7. SSO musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP
8. Możliwość uruchomienia posiadanego, skonfigurowanego i używanego przez Zamawiającego oprogramowania do backupu, aktualnie zainstalowanego na systemie operacyjnym Windows.
9. Pełna współpraca z procesorami o architekturze 64 bit
10. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
11. SSO zapewniający natywne wsparcie dla środowiska .NET Framework 4.x
12. System operacyjny musi wspierać pracę domenową.
13. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory
14. Zawarta możliwość uruchomienia roli serwera DNS
15. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory

16. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu.
17. Interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim,
18. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
19. Możliwość dokonywania bezpłatnych aktualizacji i poprawek
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
21. Zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników,
22. Mechanizmy logowania w oparciu o login i hasło,
23. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT).
24. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
25. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
26. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
27. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
28. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na

tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe).

c. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych.

29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
31. Dostarczone oprogramowanie musi być fabrycznie nowe.

Ogólne zasady oceny równoważności

1. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
2. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
3. Wykonawca zobowiązany jest podać w ofercie co najmniej nazwę producenta, nazwę oferowanego Oprogramowania, identyfikator Oprogramowania nadawany przez jego producenta, rodzaj licencji (według oznaczenia producenta), w sposób umożliwiający Zamawiającemu jednoznaczną identyfikację i weryfikację zaoferowanego Oprogramowania oraz udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.
4. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu czy licencji czasowej.
5. Zamawiający nie dopuszcza zaoferowania subskrypcji licencyjnej opartej o rozwiązania chmurowe.
6. W przypadku błędnego działania środowiska lub wykrytych niezgodności pod kątem spełnienia warunków OPZ po instalacji oprogramowania równoważnego Zamawiający ma prawo odstąpić od umowy.

Co do pozostałych równoważności to Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

Jeżeli Wykonawca chce zaproponować rozwiązanie równoważne to musi to jasno wynikać z oferty, przy czym ma również udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.

III. Oprogramowanie klasy XDR

Przedmiotem zamówienia jest dostawa licencji oprogramowania antywirusowego z usługą XDR dla 80 stacji, obejmującej okres od dostawy do 30 czerwca 2026 r.

Wykonawca dostarczy dokumenty licencyjne, warunki licencjonowania oraz klucze licencyjne i instrukcje instalacji do oprogramowania.

Oprogramowanie zaoferowane przez wykonawcę musi posiadać funkcjonalności opisane poniżej. Zamawiający dopuszcza oprogramowanie oferujące rozwiązania bardziej rozbudowane aniżeli te wskazane poniżej.

Wymagane funkcjonalności:

Administracja zdalna w chmurze

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, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi wspierać architekturę ARM64.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. 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.

10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

11. 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).

12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

13. 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.

14. 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.

15. 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.

16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• 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,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

17. 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.

18. 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.

19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.

23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

30. 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.

Ochrona serwera

1. 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, UbuntuServer 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. 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.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. 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.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

21. 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.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,

b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,

d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

7. 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.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.

3. 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.

4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.

5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.

8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.

11. 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.

12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:

a) Czysty,

b) Podejrzany,

c) Bardzo podejrzany,

d) Szkodliwy.

13. 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.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.

6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. 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.

9. 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.

10. 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.

11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

12. 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.

13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

14. 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.

15. 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.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Część druga:

Usługa wsparcia

Przedmiotem zamówienia jest usługa polegająca na opiece serwisowej oraz konfiguracji środowiska IT Zamawiającego – opisanego poniżej. Usługa będzie świadczona przez okres od podpisania umowy do 30 czerwca 2026r, w zakresie i na zasadach opisanych poniżej.

1) Opis środowiska oraz zakres wsparcia technicznego:

   1. Serwery HP DL360 Gen11:

- Diagnostyka i rozwiązywanie problemów sprzętowych: Szybka identyfikacja i eliminacja awarii komponentów (np. dyski, pamięć RAM, zasilacze, kontrolery RAID).
- Wsparcie w zakresie konfiguracji i optymalizacji: Pomoc w optymalnym ustawieniu BIOS/UEFI, konfiguracji RAID oraz aktualizacji oprogramowania układowego (firmware).

- Zarządzanie gwarancją producenta: Wsparcie w procesie zgłaszania i realizacji napraw gwarancyjnych HP.

2. Windows Server 2022/2025 Standard:

- Administracja i konfiguracja systemu operacyjnego: Pomoc w zarządzaniu rolami i funkcjami serwera (np. Active Directory, DNS, DHCP, IIS, pliki i drukarki).
- Rozwiązywanie problemów z wydajnością i stabilnością: Analiza logów systemowych, optymalizacja zasobów, usuwanie błędów systemowych.
- Zarządzanie użytkownikami i uprawnieniami: Wsparcie w tworzeniu i modyfikowaniu kont użytkowników, grup oraz polityk bezpieczeństwa (GPO).
- Aktualizacje i łatki bezpieczeństwa: Monitorowanie i aplikowanie krytycznych aktualizacji systemu.

3. Proxmox VE (Virtual Environment):

- Zarządzanie wirtualizacją: Wsparcie w tworzeniu, konfiguracji i zarządzaniu maszynami wirtualnymi (VM) oraz kontenerami (LXC).
- Optymalizacja zasobów wirtualnych: Doradztwo i pomoc w efektywnym wykorzystaniu zasobów sprzętowych serwera wirtualizacji.
- Rozwiązywanie problemów z działaniem środowiska wirtualnego: Diagnostyka i naprawa problemów z migracją VM, siecią wirtualną, czy dostępem do pamięci masowej.

4. Proxmox Backup Server:

- Konfiguracja i utrzymanie systemu backupu: Pomoc w ustawieniu harmonogramów kopii zapasowych dla maszyn wirtualnych i kontenerów.
- Weryfikacja i odzyskiwanie danych: Wsparcie w testowaniu poprawności kopii zapasowych oraz procedur odzyskiwania danych po awarii.
- Optymalizacja miejsca na dysku: Doradztwo w zarządzaniu przestrzenią dyskową na serwerze backupu.

5. Huawei Dorado 2100 (Macierz dyskowa):

- Monitorowanie i utrzymanie macierzy: Kontrola stanu dysków, kontrolerów i innych komponentów macierzy.

- Zarządzanie pulami dyskowymi i wolumenami: Wsparcie w alokacji i zarządzaniu przestrzenią dyskową dla serwerów.
- Rozwiązywanie problemów z dostępnością danych: Diagnostyka i usuwanie awarii związanych z dostępem do zasobów macierzy.

6. Aruba 6300F (Przełączniki sieciowe):

- Konfiguracja i zarządzanie siecią lokalną: Wsparcie w ustawieniu VLANów, routingu, protokołów bezpieczeństwa i zarządzania pasmem.
- Diagnostyka problemów z łącznością: Identyfikacja i rozwiązywanie problemów z siecią LAN (np. brak łączności, spadek prędkości, pętle sieciowe).
- Aktualizacje oprogramowania: Monitorowanie i instalacja najnowszych wersji oprogramowania przełączników.

7. Palo Alto 440 (Firewall):

- Konfiguracja polityk bezpieczeństwa: Pomoc w ustawieniu reguł firewall, VPN, filtrowania treści i ochrony przed zagrożeniami.
- Analiza logów i zdarzeń bezpieczeństwa: Monitorowanie i interpretacja zdarzeń w celu identyfikacji i reagowania na incydenty bezpieczeństwa.
- Wsparcie w zakresie zabezpieczeń sieciowych: Doradztwo w implementacji najlepszych praktyk w zakresie cyberbezpieczeństwa.

2) Tryb wsparcia:

- Dostępność: Poniedziałek - Piątek, w godzinach 8:00 - 16:00 lub po ustaleniu z Wykonawcą w innych godzinach.
- Zakres wsparcia: w trakcie trwania usługi Zamawiający będzie mógł skorzystać ze wsparcia Wykonawcy w wymiarze do 60 roboczogodzin.
- Tryb ustalania prac: w zakresie planowanych prac Zamawiający ustali drogą mailową lub telefoniczną przedmiot, termin zaplanowanych prac oraz szacowany czas realizacji, z co najmniej 3-dniowym wyprzedzeniem.
- Czas reakcji w przypadku awarii: gdy Zamawiający zaobserwuje nieprawidłowe działanie infrastruktury objętej wsparciem będzie miał możliwość dokonania takiego zgłoszenia Wykonawcy drogą telefoniczną lub gdy nie będzie to możliwe mailową. Reakcja na zgłoszenie nastąpi najpóźniej w przeciągu jednej godziny. W przypadku potwierdzenia awarii w funkcjonowaniu infrastruktury objętej wsparciem Wykonawca najpóźniej w dniu

następującym po zgłoszeniu przedstawi możliwe formy usunięcia awarii oraz szacowany czas realizacji. Do usunięcia awarii dojdzie najpóźniej w terminie 3 dni roboczy.

- Tryb wykonywania usługi: usługa będzie świadczona w formie zdalnej.