**Opis przedmiotu zamówienia**

Przedmiot zamówienia dotyczy dostarczenia **przedłużenia obecnie posiadanej przez  
Zamawiającego** **umowy na dostarczenie licencji oraz wsparcia technicznego** (w języku polskim i angielskim świadczonego w godzinach pracy od godziny 8 do 16 drogą telefoniczną i email) **oprogramowania Symantec Endpoint Protection** (5000 licencji pakietu ochronnego na stacje robocze i serwery (fizyczne i wirtualne) wraz z serwerem zarządzania (i konsolą) obejmujące ochronę na 3 lata (od 1 stycznia 2024 roku do 31 grudnia 2026 roku**) lub zaoferowania oprogramowania równoważnego**

Zamawiający **dopuszcza zaoferowanie oprogramowania równoważnego** - wymienionego powyżej.

Warunki równoważności (krytyczne):

1. 5000 licencji pakietu ochronnego na stacje robocze i serwery (fizyczne i wirtualne) wraz z serwerem zarządzania (i konsolą) obejmujące ochronę na 3 lata (od 1 stycznia 2024 roku do 31 grudnia 2026 roku). Zamawiający wymaga by oferta oprogramowania była wspólna zarówno dla serwerów jak i stacji roboczych i laptopów.
2. Wszystkie wymienione funkcje muszą być zawarte w jednym programie. Zamawiający nie dopuszcza rozwiązań bazujących na dodatkowych skryptach lub funkcjonalności uzupełnionej przez dodatkowe oprogramowanie
3. Dostarczone oprogramowanie nie może wymagać instalacji licencji MS CAL's oraz instalacji żadnego innego płatnego oprogramowania (Wszystkie wymagane programy oraz licencje muszą być wliczone w ofertę i nie wymagać ponoszenia dodatkowych kosztów przez zamawiającego).
4. Zamawiający wymaga by zaoferowane rozwiązanie miało ocenę nie mniejszą niż 4,4 w teście Gartnera, a producent oprogramowania musi być obecny w testach Gartnera co najmniej od roku 2018. <https://www.gartner.com/reviews/market/endpoint-protection-platforms>. Produkt nie może mieć mniejszej Rekomendacji niż 85%
5. W teście SELabs Endpoint Security Enterprise 2023: <https://selabs.uk/wp-content/uploads/2023/07/endpoint-security-eps-enterprise-2023-07-1.pdf> wskaźniki Total Accuracy Rating, Protection Accuracy,Rating, Legitimate Software Ratings, Attack Types nie mogą być mniejsze niż 100%.
6. Zamawiający nie dopuszcza zastosowania rozwiązania bazującego na serwerze oraz konsoli zarządzania w chmurze. Rozwiązanie ma bazować na serwerach zarządzających (co najmniej cztery serwery) znajdujących się na terenie Uniwersytetu Śląskiego w Katowicach.

**W przypadku zaoferowania oprogramowania równoważnego do zadań i obowiązków Wykonawcy należeć będzie:**

1. W ciągu 76 godzin od zawarcia umowy Wykonawca musi przedstawić harmonogram zmiany oprogramowania antywirusowego do akceptacji przez Zamawiającego,
2. Migrację rozpoczyna deinstalacja obecnego oprogramowania ochronnego, instalacja nowego programu ochronnego, a kończy poprawnie działający system operacyjny (a w przypadku komputerów obsługujących urządzenia zewnętrze w tym sprzęt badawczy - poprawność działania wszystkich urządzeń i sprzętu badawczego)
3. Migracja nie może powodować zakłócenia procesów dydaktycznych oraz badawczych na terenie Uniwersytetu.
4. Migracja **obecnych** serwerów zarządzania wraz z bazami danych (ustawienia komputerów, ustawienia grup, polityki firewalla, polityki antywirusa) do nowych serwerów zarządzania w terminie nie późniejszym niż **14 dni od daty** **zawarcia umowy.** Zadanie musi zostać wykonane w godzinach pracy zamawiającego tj. 8:00 – 15:00 w obecności osoby odpowiedzialnej za serwer przy wcześniejszym ustaleniu godziny migracji. Godziny migracji ustala Zamawiający / opiekun danego komputera. Zamawiający będzie wymagać pełnej odbudowy środowiska serwerowego.
5. Zamawiający wykorzystuje data mining w analizie logów. Z racji zachowania ciągłości zamawiający wymaga migracji wszystkich logów z ostatnich 160 dni zarówno aktywności programu antywirusowego jak i wszystkich zablokowanych / dopuszczonych połączeń sieciowych dla każdego komputera w terminie nie późniejszym niż **14 dni od daty** **zawarcia umowy**.
6. Migracja **wszystkich** komputerów zamawiającego z uwzględnieniem deinstalacji i instalacji nowego oprogramowania (laptopy / komputery / serwery) – do nowego oprogramowania antywirusowego w terminie nie późniejszym niż **14 dni od daty** **zawarcia umowy** roku we wszystkich placówkach zamawiającego znajdujących się w Chorzowie, Katowicach, Sosnowcu, Cieszynie. Zadanie musi zostać wykonane w godzinach pracy zamawiającego tj. 8:00 – 15:00 w dni robocze. Zainstalowane oprogramowanie musi być aktywne i w pełni funkcjonalne od czasu instalacji. Migracja musi się odbyć przynajmniej przy obecności osoby majątkowo odpowiedzialnej za komputer/serwer/laptop przy wcześniejszym ustaleniu dostępności komputera. Z racji bezpieczeństwa zamawiający nie wyraża zgody na jakiekolwiek zdalne działanie (TeamViewer / RDP) lub instalowanie jakiegokolwiek innego oprogramowania oraz jakiekolwiek zmiany miejsca użytkowania komputerów. Wszystkie komputery mają być podłączone do odpowiednich serwerów zarządzania. Środowisko zamawiającego jest środowiskiem mieszanym domenowym i lokalnym (z przewagą lokalnego). Dodatkowo wszystkie instalacje obecnego oprogramowania są zabezpieczone hasłem deinstalacyjnym. Godziny migracji ustala Wykonawca ustala z określonym użytkownikiem komputera w trakcie jego obecności przy stanowisku pracy.
7. Zamawiający korzysta z komputerów obsługujących sprzęt badawczy (mikroskopy optyczne, elektronowe, analizatory, tensometry, etc. etc.) gdzie jest zainstalowane obecne oprogramowanie ochronne (instalacja oprogramowania została uzgodniona z producentem, oprogramowanie zostało gruntowanie przetestowane). Jeżeli migracja spowoduje problem z działaniem komputera obsługującego sprzęt badawczy / działaniem sprzętu badawczego wówczas koszty związane z wezwaniem i pracą serwisu lub wysłaniem sprzętu do siedziby producenta sprzętu badawczego pokrywa wykonawca. Zamawiający w ciągu 48 godzin od wystąpienia awarii wskaże odpowiedni autoryzowany serwis sprzętu badawczego. Wykonawca musi w ciągu 24 godzin wezwać odpowiedni serwis i powiadomić o tym fakcie Zamawiającego. Wszystkie dodatkowe koszty związane z zatrzymaniem procesu badawczego (przeterminowanie odczynników, utrata próbek, utrata właściwości badawczych obiektu) pokrywa Wykonawca. Zamawiający z racji poufności badań naukowych nie zgadza się na wykonywanie kopii zapasowych na jakichkolwiek dyskach USB.
8. Wykonawca bezwzględnie zapewni wsparcie techniczne w przypadku niepowodzenia operacji przejścia na nowy program antywirusowy dla każdej maszyny / serwera / serwera wirtualnego. Obowiązkiem wsparcia technicznego jest doprowadzenie maszyny / serwera / serwera wirtualnego do pełnej funkcjonalności przed zainstalowaniem nowego programu antywirusowego (Wdrożenie odbywa się będzie w środowisku klientów zabezpieczonych hasłem) oraz znalezienie rozwiązania problemu instalacji – tak by każdy komputer lub serwer posiadał zainstalowane oprogramowanie ochronne. Zadanie musi zostać wykonane w czasie pracy zamawiającego tj. od 8:00 do 15:00 i nie może trwać dłużej niż 16 godzin roboczych. **W przypadku niepowodzenia całego procesu migracji w wyznaczonym terminie (14 dni od daty zawarcia umowy) Wykonawca zobowiązany jest przywrócić całe zmigrowane środowisko do stanu przed migracją (ponowna instalacja serwerów i klientów Symantec) oraz zapewnić ochronę Zamawiającego na aktualnych warunkach poprzez przedłużenie czasu trwania aktualnie funkcjonującego rozwiązania.**
9. W przypadku gdy instalacja oprogramowania spowoduje problem z dostępem do danych Wykonawca w ciągu 48 godzin od wystąpienia problemu zaproponuje sposób odzyskania danych, również z uwzględnieniem tj. przesłania komputera lub dysku do specjalistycznego laboratorium odzysku danych jeżeli przy wdrożeniu doszło do naruszenia struktury, braku dostępu lub utraty danych. Z racji bezpieczeństwa danych zamawiający określi firmę do jakiej zostanie wysłany dysk. Wszystkie koszty odzyskania danych są w kwestii Wykonawcy;
10. **Funkcjonalność fakultatywna:** Zaoferowanie funkcjonalności sandbox na maszynach wirtualnych zamawiającego / w infrastrukturze zamawiającego lub w chmurze producenta. Serwer sandbox musi działać niezależnie od serwera zarządzającego i nie wymagać posiadania serwera zarządzania w chmurze. W przypadku zaoferowania funkcjonalności sandbox w chmurze producenta, Zamawiający nie wyraża zgody, by serwer sandbox znajdował się poza terytorium USA / UE. Zamawiający musi mieć możliwość określenia, jakie typy plików są wysyłane na serwer i mieć możliwość odrzucenia sugestii wysłania pliku na serwer.
11. Przeprowadzenia szkolenia on-line obejmującego zagadnienia konfiguracji środowiska klienckiego oraz serwerowego dla grupy min. 30 osób ze środowiska IT zamawiającego. Dodatkowo:
    * + - 1. Przyjęte rozwiązanie do prowadzenia nie może wymagać instalacji jakiegokolwiek oprogramowania na komputerach osób uczestniczących w szkoleniach oraz musi umożliwiać komunikację głosową w obie strony (prezenter oraz pytania do prezentacji).
          2. Szkolenie musi odbywać się w czasie rzeczywistym, zamawiający nie dopuszcza stosowania nagranych wcześniej filmów
          3. Trenerem ma być osoba spełniająca następujące wymagania: jeden certyfikat wydany przez producenta oprogramowania i co najmniej w ciągu ostatnich 12 miesięcy przeprowadziła 6 szkoleń.
          4. Szkolenie musi obejmować wszystkie aspekty proponowanego rozwiązania i musi trwać co najmniej 20 godzin w sumie. Zamawiający w porozumieniu z Wykonawcą przygotuje odpowiedni terminarz spotkań
          5. Wykonawca przygotuje dokumenty / certyfikaty poświadczające udział w szkoleniu.
          6. Uczestnicy szkolenia będą mogli przez co najmniej 30 dni zadawać dodatkowe pytania do trenera, czas odpowiedzi nie może być dłuższy niż 5 dni roboczych
          7. Minimalny program szkolenia: funkcjonalność serwera, zarządzanie grupami, politykami i uprawnieniami, polityki, zadania agenta i serwera, ochrona antywirusowa i firewall, kontrola dostępu aplikacji i urządzeń, rozwiązywanie problemów, aktualizacja online / offline
          8. Plan szkolenia musi zostać przedstawiony do akceptacji do 76 godzin od zawarcia umowy
          9. Cykl szkoleń musi rozpocząć się w terminie do 14 dni od daty zawarcia umowy.
          10. Wszelkie koszty związane z przeprowadzeniem szkoleń są ponoszone przez Wykonawcę.

**Warunki równoważności, minimalne warunki techniczne produktu:**

**Ochrona antywirusowa:**

1. Usuwanie wirusów, makro–wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware” i „adware”, włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu.
2. Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym.
3. Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie,
4. Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane
5. Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych,
6. Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:
7. na dyskach twardych
8. w boot sektorach
9. na zewnętrznych dyskach twardych (np. podłączonych przez port USB)
10. Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej
11. Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
12. Scentralizowaną obsługę wirusów polegającą na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań
13. Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek
14. Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, Rich Text Format,
15. Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej
16. Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące
17. Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zastawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów
18. Możliwość natychmiastowego wymuszenia aktualizacji definicji wirusów na stacjach klienckich i serwerach.
19. Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 3 razy dziennie
20. Aktualizacja baz definicji musi być aplikowana tylko w czasie nieaktywności użytkownika na komputerze – jeżeli użytkownik komputera na nim pracuje, aplikacja automatycznie zostaje opóźniona
21. Możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę
22. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów
23. Dedykowany moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger – analiza zachowania opiera się na wykonywanych przez aplikację czynnościach (tworzenie nowych plików, komunikacja z Internetem, podmiana strony w przeglądarce, itp.). Schematy szkodliwego działania powinny być generowane w procesie uczenia maszynowego (Machine Learning) zaimplementowanego na sieci składającej się z co najmniej 150milionów sond.
24. Dedykowany moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie
25. Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.
26. Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
27. Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe
28. Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione
29. Skanowanie poczty klienckiej (na komputerze klienckim)
30. Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach
31. Ściągnięcie dowolnego pliku na komputer musi spowodować sprawdzenie reputacji takiego pliku – jako reputacja rozumie się odpowiedź, co do ilość użytkowników w Internecie korzystających z danej aplikacji/pliku, czasu, kiedy aplikacja/plik pojawiła się w Internecie po raz pierwszy, oraz czy aplikacja/plik jest „dobra” czy też nie
32. System musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikacje, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 5, 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni
33. W Windows 8 i Windows 10 wsparcie dla funkcji ELAM (Early Launch Anti-Malware) poprzez dostarczenie odpowiedniego sterownika ELAM.
34. Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.
35. Dla systemów typu Windows Embedded wsparcie dla Windows Embedded write filters w tym dla File-Based Write Filter (FBWF)
36. Możliwość wyboru wielkości definicji antywirusowych, z której będzie korzystał zainstalowany agent – system musi posiadać pełna wersję sygnatur oraz ich wersję uproszczoną znacząco mniejszą od pełnej do instalacji na systemach z niewielką ilością miejsca na dyskach oraz w systemach VDI.
37. System musi posiadać możliwość emulacji w celu analizy polimorficznego złośliwego oprogramowania.
38. System musi być wyposażony w dynamiczny klasyfikator próbek wykorzystujący mechanizmy uczenia maszynowego (Machine Learning) w celu wykrywania nowych wersji znanych rodzin złośliwego oprogramowania. Zbiór danych wykorzystywany w algorytmach uczących musi pochodzić z sieci składającej się z co najmniej 150mln sond. Musi istnieć możliwość konfiguracji agresywności (czułości) mechanizmu Machine Learning zarówno w zakresie poziomu, powyżej którego zostanie zgłoszony alarm jak również w zakresie poziomu, powyżej którego system podejmie akcje remediacyjne.

**Zapora ogniowa – system Firewall**

1. Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.
2. Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe,
3. Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać,
4. Administrator może konfigurować dostęp stacji do protokołów rozszerzonych innych niż ICMP,UDP czy TCP np.: IGMP, GRE, VISA, OSPFIGP, L2TP, Lite-UDP,
5. Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne
6. Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli
7. Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji
8. Konfiguracja stacji ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji dns (FQDN) lub domeny dns
9. Firewall powinien umożliwiać nagrywanie komunikacji spełniającej wskazane wymagania.
10. Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.
11. W przypadku wykrycia zdefiniowanego ruchu, firewall ma wysłać wiadomość do administratora
12. Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www
13. Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację
14. Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP
15. Domyślne reguły zezwalające na ruch DHCP, DNS, WINS

**System IPS**

1. Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez system. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie.
2. Biblioteka ataków i podatności musi zawierać przynajmniej 4500 sygnatur( z włączeniem programów P2P). System ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort’a. Sygnatury te mogą działać w trybie blokuj lub rejestruj.
3. Wykrywanie trojanów i generowanego przez nie ruchu
4. Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.
5. Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków
6. System ochrony przed włamaniami musi automatycznie integrować się z przeglądarką internetową (przynajmniej z Internet Explorer oraz Firefox) – uniemożliwiając wykonanie w nich (nawet, jeżeli są podatne) szkodliwego dla nich kodu
7. System musi posiadać mechanizm blokowania wykorzystywania nieznanych podatności w określonym oprogramowaniu (Exploit Prevention) co najmniej dla aplikacji pakietu Office, Firefox, Internet Explorer oraz aplikacji napisanych w języku Java a także VLC. System musi implementować co najmniej 10 technik ochrony w tym następujące metody prewencji:
   1. Java Exploit Protection
   2. Structured Exception Handling Overwrite Protection (SEHOP)
   3. Heap Spray Memory Attack
   4. Forced DEP
   5. Forced ASLR
   6. Anti-ROP

**Ochrona systemu operacyjnego**

1. System ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji
2. System ma umożliwiać ładownie modułów lub bibliotek DLL
3. System ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje (aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową)
4. System ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym
5. System ma kontrolować dostęp do rejestru systemowego
6. System ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne
7. System musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych
8. Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu
9. Możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego
10. Możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji systemuw taki sposób, by żadna inna aplikacja/biblioteka z poza listy nie mogła uruchomić się na komputerze
11. Kolekcja aktualnie znajdujących się aplikacji na systemie końcowym musi być możliwa do wywołania bezpośrednio z konsoli zarządzającej – bez konieczności wykonania jakichkolwiek czynności na systemie końcowym
12. Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji systemu w taki sposób, by tylko aplikacja znajdujące się na liście nie mogły uruchomić się na komputerze
13. Możliwość automatycznego importu list zarówno białej, jaki i czarnej, co zdefiniowany interwał czasu

**Mechanizm pułapek:**

1. System musi posiadać wbudowany mechanizm pułapek pozwalający na detekcję zaawansowanych ataków poprzez obserwowanie sztucznie wytworzonych zasobów - przynęt.
2. System powinien umożliwiać zdefiniowanie następujących przynęt:
   1. Użytkownika – przynętą są sztucznie spreparowane informacje uwierzytelniające dla użytkownika. Każda próba użycia tych informacji uwierzytelniających powinna generować alarm.
   2. Proces – przynęta imituje działanie procesu innego systemu ochrony. Każda próba zatrzymania sztucznego procesu powinna generować alarm.
   3. Udział sieciowy – powinna wykrywać próby połączenia z nieistniejącym, ale specjalnie spreparowanym udziałem sieciowym. Każda próba dostępu do udziału powinna generować alarm.
   4. IP – przynęta polegająca na sztucznym wstrzyknięciu do systemu operacyjnego informacji o nieistniejącym adresie IP. System powinien wygenerować alarm w przypadku próby połączenia z adresem-przynętą.
   5. DNS – przynęta polegająca na wstrzyknięciu w system operacyjny sztucznej domeny. Każda próba dostępu do tej domeny powinna generować alarm.
3. System powinien samodzielnie ustawiać i usuwać przynęty w zależności od konfiguracji polityki. Konfiguracja powinna być dostępna z interfejsu administracyjnego rozwiązania.
4. Mechanizm pułapek powinien mieć wspólny panel raportowania z pozostałymi elementami systemu.

**Integralności komputera:**

1. Oprogramowanie musi umożliwiać wykonywanie szerokiego zakresu testów integralności komputera pod kątem zgodności z polityką bezpieczeństwa urządzeń końcowych, w tym: programów antywirusowych, poprawki firmy Microsoft, dodatki Service Pack firmy Microsoft, osobistych zapór ogniowych
2. Testy integralności ma być przeprowadzany cyklicznie, co zdefiniowany okres czasu.
3. Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta
4. Oprogramowanie musi umożliwiać wykonanie niestandardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać zaawansowaną składnie If…Then…Else.
5. W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:
6. Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne
7. Pliki - istnienie, data, rozmiar, suma kontrolna
8. Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego
9. Zainstalowane poprawki
10. Uruchomiony proces, wersja systemu operacyjnego
11. Własny skrypt VisualBasic, wsh, itp.
12. Własna aplikacja
13. W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako możliwe operacje do wykonania, musi istnieć możliwość:
14. Uruchamianie dowolnego/własnego skryptu lub programu
15. Logowanie zdarzenia
16. Ukazanie okienka z wiadomością
17. Pobieranie oraz uruchamianie instalacji
18. Ma istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.
19. Możliwość wymuszenia instalacji dowolnej aplikacji.
20. W wypadku niezgodności własnego systemu, oprogramowanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.
21. Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.
22. Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.
23. Musi istnieć test integralności komputera, który sprawdzi czy komputer nie jest podłączony do Internetu poprzez dwie różne drogi, np. poprzez kabel sieciowy (Ethernet) i poprzez dostęp mobilny (WIFI, modem GSM, etc.)

**Ochrona środowisk wirtualnych**

1. System musi umożliwiać identyfikacje środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Citrix, Microsoft, VMWare
2. System musi umożliwiać w wypadku skanowania w czasie rzeczywistym oraz przy skanowaniu zaplanowanym, wykluczenie w środowisku wirtualnym wszystkich plików z tzw. złotego obrazu (Gold Image) - nie będą one nigdy poddawane skanowaniu
3. System musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym. Technologia ta powinna być dostępna, jako oprogramowanie instalowane w systemie operacyjnym Windows
4. System musi umożliwiać prawidłowe rozliczenia licencji oferowanego systemu dla systemów wirtualnych typu desktop tzw. VDI, w szczególności tzw. „non-persistent”
5. System musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń

**Architektura**

1. Rozwiązanie ma mieć architekturę trój-warstwową. Klienci mają być zarządzani przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.
2. Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.
3. Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.
4. Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.
5. Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
6. Serwery zarządzające mają móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).
7. Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostarczyciela aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.
8. Definiowanie lokalnego repozytorium musi zawierać warunki, jakie muszą być zachowane by dany komputer mógł stać się lokalnym repozytorium – warunkami muszą być przynajmniej: wersja systemu operacyjnego, adres komputera, nazwa komputera (z możliwością podania ją ze znakami specjalnymi, np.: komputer\*), określonego wpisu w rejestrze.
9. Możliwość manualnego wskazania wybranej grupie komputerów konkretnego lokalnego dostarczyciela aktualizacji.
10. Możliwość uruchomienia dedykowanego narzędzia służącego do monitorowania klientów, którzy zostali lokalnymi dostarczycielami aktualizacji. Monitorowane jest ich zdrowie, ilość ściągniętych od nich danych, czy były to ściągnięte pełne definicje czy też definicje przyrostowe.
11. Możliwość ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.

**Wymagania serwer:**

Środowisko pracy serwera: Windows Server 2016 – 2022, możliwość tworzenia współistniejących niezależnych serwerów z wzajemną replikacją, baza danych nie może wymagać zakupu dodatkowych licencji dostępowych i posiadać rozwiązanie umożliwiające pobieranie danych bezpośrednio z bazy. Dodatkowo:

1. Klient dla system Mac i Linux ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows. Dodatkowo serwer musi posiadać możliwość utworzenia innego dedykowanego wyłącznie celom raportowym serwisu www.
2. Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli
3. Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci,
4. System ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji systemu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.
5. System ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. System ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.
6. Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami
7. Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
8. Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
9. Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
10. Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.
11. Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
12. Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory. System ma mieć możliwość wykorzystania wielo-elementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.)
13. Dostęp do interfejsu systemu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
14. Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.
15. Lokalizacja ma być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.
16. Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I” oraz „LUB” na powyżej wymienionych elementach.
17. Paczki instalacyjne systemu mają pozwalać na dodanie własnej konfiguracji
18. W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji obecnego systemu

bezpieczeństwa, która uruchomi się automatycznie przed instalacją systemu.

1. Funkcjonalność musi uwzględniać to, że deinstalacja obecnego systemu wymaga podania hasła.
2. Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym
3. Nowe wersje oprogramowania mają być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.
4. System ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.
5. Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:
6. błędnej autoryzacji do systemu zarządzania
7. dostępności nowego oprogramowania
8. pojawienia się nowego komputera
9. zdarzeń powiązanych z infekcjami wirusów
10. stanu serwerów zarządzających
11. Możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji
12. Oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający
13. Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

**Wymagania klienci:**

Środowisko pracy (wszyscy klienci raportują do lub większej liczby serwerów. W przypadku awarii jednego z serwerów klient ma automatycznie raportować lub pobierać polityki z awaryjnego serwera. Zamawiający nie dopuszcza oddzielnych serwerów dla różnych systemów operacyjnych klasy Linux, Windows i MACOS) (WARUNEK KRYTYCZNY).

Klient musi mieć możliwość w pełni konfigurowalnego ustawienia wyjątków (ustawienie poziomu dostępów do określonych opcji wyjątków z poziomu serwera).

Zamawiający wymaga zapewnienia wolnego dostępu do programu deinstalującego wszystkie składniki klienta.

Wspierane systemy operacyjne:

* MS Windows 10 / 11 / 2008 / 2012 / 2012r2 / 2016 / 2019 / 2022 / 7 / 8.1
* Linux (Ubuntu, Fedora Core, Debian, Mint, SUSE Linux Enterprise Desktop, SUSE Linux Enterprise Server, Red Hat Enterprise Linux Server)
* MACOS (Mac OS X, 10.11, macOS 10.12, macOS 10.13, macOS 10.14 macOS 10.15)

Inne wymagania:

1. Szyfrowania komunikacja pomiędzy klientem a serwerem (obustronna) z możliwością konfiguracji portu komunikacyjnego;
2. Możliwość zmiany serwera raportującego w kliencie bez konieczności deinstalacji programu ochronnego;
3. Blokada (hasłem) deinstalacji, zatrzymania programu ochronnego lub jakiegokolwiek komponentu z poziomu panelu sterowania lub aplikacji producenta do wyinstalowania programu ochronnego;
4. Baza danych umożliwiająca swobodny dostęp dla administratora! (konfiguracja raportów niezależnych od serwera i systemu zarządzania programem ochronnym z poziomu bazy danych);
5. Dowolna konfiguracja portów komunikacyjnych serwer – klient;
6. Dostęp do konsoli z strony www i RDP (lub innego klienta);
7. Wbudowane zabezpieczenie serwera (biała lista dostępów IP ipv4 i ipv6);