|  |
| --- |
| Przedmiot zamówienia - wymagania Zamawiającego **Licencja na oprogramowanie do ochrony 700 urządzeń na okres 12 miesięcy**  **CENTRALNE ZARZĄDZANIE**   1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. 8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 9. Rozwiązanie musi zapewniać weryfikację 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). 10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 12. Rozwiązanie musi zapewniać tworzenie grup statycznych i dynamicznych komputerów. 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. 13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 14. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.   **OCHRONA STACJI ROBOCZYCH**   1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10), LINUX (Ubuntu Desktop 18.04 / 20.04 LTS 64-bit, Red Hat Enterprise Linux 7 64-bit, SUSE Linux Enterprise Desktop) oraz MacOS (10.12 lub nowsze) 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 3. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 5. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 8. 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. 9. 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). 10. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 11. 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. 12. 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. 13. 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. 14. Rozwiązanie musi posiadać Moduł HIPS pracujący w jednym z pięciu trybów:     1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,     2. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,     3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,     4. tryb uczenia się, w którym program 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,     5. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 15. Rozwiązanie musi posiadać wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, 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. 16. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 17. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 18. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 19. Rozwiązanie musi posiadać zintegrowany moduł kontroli dostępu do stron internetowych w opraciu adresy URL dostarczane i automatycznie aktualizowane przez producenta oraz podzielone na co najmniej 140 kategoriach i podkategoriach z uwzględnieniem co najmniej: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 20. Rozwiązanie musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. 21. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki. 22. Rozwiązanie musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika w bezpiecznej przeglądarce 23. Rozwiązanie musi zapewniać w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, automatyczne przekierowanie do okna bezpiecznej przeglądarki. 24. Rozwiązanie musi posiadać możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. 25. Rozwiązanie musi posiadać ochronę antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. 26. Rozwiązanie musi wspierać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 27. Rozwiązanie musi zapewniać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. 28. Rozwiązanie musi zapewniać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. 29. Rozwiązanie musi zapewniać możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.   1. Rozwiązanie musi posiadać zaporę osobistą pracującą w jednym z czterech trybów:   * + tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,   + tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,   + tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,   + tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.  1. Rozwiązanie musi oceniać reguły zapory systemu Windows. 2. Rozwiązanie musi wspierać określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. 3. Rozwiązanie musi zapewniać tworzenie profili pracy zapory osobistej w zależności od wykrytej sieci. 4. Rozwiązanie musi zapewniać możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. 5. Rozwiązanie musi posiadać możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. 6. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Rozwiązanie musi pozwalać na rozwiązanie problemów:  * z aplikacją lokalną, którą administrator wskazuje z listy, * z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.  1. Rozwiązanie musi posiadać moduł szyfrowania całej powierzchni dysków. 2. Rozwiązanie musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Rozwiązanie musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 3. Rozwiązanie musi wspierać wykorzystanie modułu TPM. 4. Rozwiązanie musi wspierać korzystanie z technologii TCG OPAL - dyski sprzętowo szyfrowane. 5. Rozwiązanie musi zapewniać zarządzanie z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej. 6. Rozwiązanie musi zapewniać możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:   a) ilość znaków,  b) czy hasło ma zawierać wielkie litery,  c) czy hasło ma zawierać małe litery,  d) czy hasło ma zawierać cyfry,  e) czy hasło ma zawierać znaki specjalne,  f ) okres ważności,  g) ilość nieudanych logowań,  h) możliwość zmiany hasła.   1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day wykorzystujące działanie chmury producenta 2. Rozwiązanie musi posiadać możliwość wstrzymania otwarcia pliku przez użytkownika przed wykonaniem analizy. 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. Rozwiązanie musi posiadać opcję zdefiniowania po jakim czasie przesłane pliki zostaną usunięte z serwerów producenta. 5. Rozwiązanie musi posiadać możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 8. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 9. Rozwiązanie musi zapewniać odpowiednie oznaczenie dla przeanalizowanych próbek. Analiza pliku może zakończyć się z wynikiem:    1. Czysty,    2. Podejrzany,    3. Bardzo podejrzany,    4. Szkodliwy.   **OCHRONA SERWERA PLIKÓW**   1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych, 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 posiadać wbudowaną technologię do ochrony przed rootkitami i exploitami. 5. System antywirusowy musi wspierać wykorzystywanie wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 6. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 7. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 8. 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. 9. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 10. Rozwiązanie musi posiadać możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 11. 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. 12. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 13. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 14. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 15. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 16. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* 17. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 18. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. 19. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 20. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.   **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:    1. usunięcie zawartości urządzenia,    2. przywrócenie urządzenie do ustawień fabrycznych,    3. zablokowania urządzenia,    4. uruchomienie sygnału dźwiękowego,    5. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: 8. nazwę aplikacji, 9. nazwę pakietu, 10. kategorię sklepu Google Play, 11. uprawnienia aplikacji, 12. pochodzenie aplikacji z nieznanego źródła. |