|  |
| --- |
| OPIS PRZEDMIOTU ZAMÓWIENIA – Zadanie nr 1 |
| **System EDR** (Endpoint Detection and Response) |

04/ZP/2022

Uwagi i objaśnienia:

* Parametry określone jako „tak” są parametrami granicznymi. Udzielenie odpowiedzi „nie” lub innej nie stanowiącej jednoznacznego potwierdzenia spełniania warunku będzie skutkowało odrzuceniem oferty.

**PARAMETRY TECHNICZNE I EKSPLOATACYJNE**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | PARAMETR | **PARAMETR WYMAGANY** | **Parametr oferowany (podaje Wykonawca)** |
|  | **System zaawansowanej ochrony antywirusowej stacji roboczych, serwerów, wyposażony w funkcję szyfrowania dysków oraz Endpoint Detection and Response (EDR), spełniający poniższe funkcje: 150 stanowisk na min. 2 lata. Należy dostarczy również system operacyjny na którym będzie zainstalowane oprogramowanie.** | **TAK** |  |
| 1.1. | 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. | TAK |  |
| 1.2. | Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. | TAK |  |
| 1.3. | Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. | TAK |  |
| 1.4. | Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. | TAK |  |
| 1.5. | Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. | TAK |  |
| 1.6. | 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. | TAK |  |
| 1.7. | Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. |  |  |
| 1.8. | Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. | TAK |  |
| 1.9. | 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). | TAK |  |
| 1.10. | Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. | TAK |  |
| 1.11. | Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. | TAK |  |
| 1.12. | Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. | TAK |  |
| 1.13. | 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. | TAK |  |
| 1.14. | Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. | TAK |  |
| 1.15. | Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. | TAK |  |
| 1.16. | Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. | TAK |  |
| 1.17. | Rozwiązanie musi informować administratora o nieaktualnych komponentach w tym przynajmniej JAVA i serwer SQL. |  |  |
|  | **Ochrona stacji roboczych** | TAK |  |
| 2.1. | Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows8.1/Windows 10/Windows 11), MacOS 10.15 lub nowszy. | TAK |  |
| 2.2. | Rozwiązanie musi wspierać architekturę ARM64. | TAK |  |
| 2.3. | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. |  |  |
| 2.4. | Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. | TAK |  |
| 2.5. | Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | TAK |  |
| 2.6. | Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | TAK |  |
| 2.7. | Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. | TAK |  |
| 2.8. | Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. | TAK |  |
| 2.9. | 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. | TAK |  |
| 2.10. | 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). | TAK |  |
| 2.11. | Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. | TAK |  |
| 2.12. | 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. | TAK |  |
| 2.13. | 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. | TAK |  |
| 2.14. | 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. | TAK |  |
| 2.15. | 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. | TAK |  |
| 2.16. | 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. | TAK |  |
| 2.17. | 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. | TAK |  |
| 2.18. | Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. | TAK |  |
| 2.19. | Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). | TAK |  |
| 2.20. | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | TAK |  |
| 2.21. | Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. | TAK |  |
| 2.22. | 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. | TAK |  |
| 2.23. | Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. | TAK |  |
| 2.24. | Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. | TAK |  |
| 2.25. | Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. | TAK |  |
| 2.26. | Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. | TAK |  |
| 2.27. | Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. | TAK |  |
| 2.28. | Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. | TAK |  |
| 2.29. | 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. | TAK |  |
| 2.30. | Rozwiązanie musi wykorzystywać do działania chmurę producenta (Sandbox w chmurze). | TAK |  |
| 2.31. | 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. | TAK |  |
| 2.32. | Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. | TAK |  |
| 2.33. | Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. | TAK |  |
| 2.34. | Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. | TAK |  |
|  | **Ochrona serwera** |  |  |
| 3.1. | Rozwiązanie musi wspierać systemy Microsoft Windows Server 2008 R2 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux. | TAK |  |
| 3.2. | Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. | TAK |  |
| 3.3. | Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | TAK |  |
| 3.4. | Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. | TAK |  |
| 3.5. | 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. | TAK |  |
| 3.6. | Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. | TAK |  |
| 3.7. | Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. | TAK |  |
| 3.8. | Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. | TAK |  |
| Dodatkowe wymagania dla ochrony serwerów Windows: | |  |  |
| 3.9. | Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. | TAK |  |
| 3.10. | Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). | TAK |  |
| 3.11. | Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. | TAK |  |
| 3.12. | Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | TAK |  |
| 3.13. | 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. | TAK |  |
| 3.14. | Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. | TAK |  |
| 3.15. | Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* | TAK |  |
| 3.16. | Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | TAK |  |
| 3.17. | Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. | TAK |  |
| Dodatkowe wymagania dla ochrony serwerów Linux: | |  |  |
| 3.18. | Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. | TAK |  |
| 3.19. | Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. | TAK |  |
| 3.20. | Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. | TAK |  |
| 3.21. | 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. | TAK |  |
|  | **Szyfrowanie** | TAK |  |
| 4.1. | System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. | ~~TAK~~ |  |
| 4.2. | System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). | TAK |  |
| 4.3. | 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. | TAK |  |
| 4.4. | Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. | TAK |  |
|  | **Endpoint Detection and Response** | TAK |  |
| 5.1. | Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta. | TAK |  |
| 5.2. | Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. | TAK |  |
| 5.3. | Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. | TAK |  |
| 5.4. | Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. | TAK |  |
| 5.5. | Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”. | TAK |  |
| 5.6. | Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia. | TAK |  |
| 5.7. | Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. | TAK |  |
| 5.8. | Rozwiązanie musi umożliwić administratorowi weryfikację 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. | TAK |  |
| 5.9. | Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania. | TAK |  |
| 5.10. | Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł. | TAK |  |
| 5.11. | Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli. | TAK |  |
| 5.12. | Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell. | TAK |  |
|  | **Ochrona urządzeń mobilnych opartych o system Android** | TAK |  |
| 6.1. | Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. | TAK |  |
| 6.2. | Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. | TAK |  |
| 6.3. | Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). | TAK |  |
| 6.4. | Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. | TAK |  |
| 6.5. | 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. | TAK |  |
| 6.6. | Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. | TAK |  |
| 6.7. | Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:   1. nazwę aplikacji, 2. nazwę pakietu, 3. kategorię sklepu Google Play, 4. uprawnienia aplikacji, 5. pochodzenie aplikacji z nieznanego źródła. | TAK |  |