*Załącznik nr 3 do SWZ*

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

|  |  |
| --- | --- |
| **L.p.** | **ROZBUDOWA SYSTEMU OCHRONY URZĄDZEŃ** |
|  | ***Moduły wymagane*** |
|  | **Informacje ogólne** |
|  | Istniejący system ochrony urządzeń ESET należy rozbudować o narzędzia bezpieczeństwa, minimum w zakresie funkcjonalności umożliwiającej wykrywanie incydentów i automatyczne reagowania umożliwiającego korelację zdarzeń (XDR).  Nr licencji obecnie posiadanego systemu 33B-RCA-5EB |
|  | W wyniku rozbudowy systemu o nowe moduły funkcjonalne przy zachowaniu dotychczasowej funkcjonalność w zakresie ochrony stacji roboczych, ochrony serwerów, ochrony urządzeń mobilnych. Nowe moduły muszą być kompatybilne z istniejącym systemem, a całe rozwiązanie musi zapewniać minimum funkcjonalność określoną w pkt. 2 - 6 |
|  | Zamawiający dopuszcza wymianę istniejącego rozwiązania na rozwiązanie równoważne do istniejącego systemy ochrony urządzeń, realizującego minimum funkcjonalności opisane w pkt.2-6, Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wy specyfikowanego.  Dostarczenie przez wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana systemu na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania Oprogramowania w środowisku produkcyjnym itp. |
|  | Rozwiązanie musi zapewniać ochronę 250 stacji komputerowych w poniższym zakresie. |
|  | **Wymagania ogólne** |
|  | Rozwiązanie musi być zarządzane z jednej centralnej konsoli administracyjnej dostępnej z poziomu interfejsu WWW zabezpieczonego protokołem SSL. Wymagana jest autoryzacja dwuetapowa do konsoli administracyjnej. |
|  | Serwer administracyjny dostępny w chmurze musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci oraz musi umożliwiać tworzenie polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. |
|  | Konsola administracyjna 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. |
|  | Uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. |
|  | **XDR** |
|  | Automatyczna wizualizacja zdarzeń, incydentów i ataków ukierunkowanych |
|  | Możliwość wyszukiwania zagrożeń na podstawie definiowanych filtrów |
|  | Wbudowany zestaw reguł zapewniający reagowanie na wykryte incydenty z możliwością budowania własnych reguł oraz edycji istniejących. |
|  | Możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. |
|  | Możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa |
|  | Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. |
|  | Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. |
|  | Możliwość uruchomienia reguł w oparciu o dane historyczne. |
|  | Możliwość blokowania plików po sumach kontrolnych. |
|  | Możliwość ustawiania priorytetu zdarzeń. |
|  | 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. |
|  | Możliwość oznaczenia plików DLL jako bezpieczne, pobrania do analizy oraz ich zablokowania. |
|  | Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. |
|  | Dla wykonanego skryptu lub pliku exe, weryfikacja powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. |
|  | Możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). |
|  | Możliwość włączenia izolacji komputera od sieci. |
|  | **Ochrona stacji roboczych** |
|  | Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. |
|  | Ochrona przed rootkitami oraz podłączeniem komputera do sieci botnet. |
|  | Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. |
|  | Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. |
|  | Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. |
|  | Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. |
|  | Umieszczenia na liście wykluczeń wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. |
|  | 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). |
|  | Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. |
|  | 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. |
|  | 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. |
|  | Blokowanie nośników wymiennych, bądź grup urządzeń wraz z możliwością tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. |
|  | Możliwość generowania raportu dotyczącego stacji, zawierającego informacje dotyczące, minimum: zainstalowanych aplikacji, usług systemowych, systemu operacyjnego, aktywnych procesów, połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. |
|  | Automatyczna, inkrementalna aktualizacja silnika detekcji. |
|  | Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). |
|  | Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. |
|  | Zintegrowany moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika. |
|  | Zintegrowany moduł kontroli dostępu do stron internetowych. |
|  | Możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. |
|  | Ochrona przed zagrożeniami 0-day. |
|  | **Ochrona serwerów** |
|  | Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. |
|  | Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. |
|  | Skanowania dysków sieciowych typu NAS. |
|  | Wbudowane minimum 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. |
|  | Automatyczna, inkrementalna aktualizacja silnika detekcji. |
|  | Możliwość wykluczania ze skanowania procesów. |
|  | Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. |
|  | System zapobiegania włamaniom działający na hoście (HIPS). |
|  | Skanowanie magazynu Hyper-V. |
|  | Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. |
|  | Możliwość blokowania zewnętrznych nośników danych na serwerze 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. |
|  | Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. |
|  | Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. |
|  | Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. |
|  | Możliwość uruchomienia lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. |
|  | **Ochrona urządzeń mobilnych** |
|  | Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. |
|  | Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). |
|  | Możliwość skonfigurowania zaufanej karty SIM. |
|  | Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. |
|  | Wyświetlenie listy zainstalowanych aplikacji. |
|  | Blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła. |
|  | **Instalacja i Konfiguracja** |
|  | Zamawiający wymaga instalacji dostarczonych rozwiązań na urządzeniach wskazanych przez zamawiającego na etapie realizacji. |
|  | Należy skonfigurować moduł XDR i zoptymalizować reguły reagowania na incydenty oraz przygotować polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem wraz z uruchomieniem konsoli chmurowej. |
|  | Zamawiający wymaga grupowego instruktażu technicznego prowadzonego w formie przy stanowiskowej, w siedzibie Zamawiającego, dla 4 osobowej grupy administratorów Zamawiającego w zakresie obsługi dostarczonego rozwiązania, w ilości minimum 5 godzin niezbędnych do osiągnięcia kompletnych umiejętności w zakresie wykonywania czynności administracyjnych, instalacji oprogramowania systemowego i narzędziowego, znajomości i umiejętności realizacji procedur, znajomości wytycznych polityk bezpieczeństwa. Osoby wytypowane do szkolenia w formie instruktarzu muszą poznać typowe zagrożenia i problemy związane z funkcjonowaniem systemu, a także sposoby ich wykrywania oraz przeciwdziałania. |
|  | Dodatkowo w przypadku rozwiązania równoważnego:   1. przygotować pakiety instalacyjne i zainstalować system na wszystkich stacjach komputerowych; 2. przygotować wymagane polityki dla organizacji i działu IT; 3. skonfigurować polityki szyfrowania; 4. uruchomić wszystkie moduły; 5. włączenie domyślnych reguł zgodnie z wytycznymi Zamawiającego określonymi na etapie realizacji; 6. wykonać dokumentację zawierającą opis wszystkich modułów, punktów konfiguracji(wraz z rzutami ekranowymi, adresacjami, loginami wraz z hasłami, zalecenia wdrożeniowe i przekazać minimum w formie elektronicznej; 7. zapewnienie minimum 16 godzin instruktażu stanowiskowego dla administratorów Zamawiającego zapewniającego pełne zrozumienie instalacji, konfiguracji i wdrażania rozwiązania równoważnego, potwierdzonego protokołem z wykonania instruktażu. |
|  | **Dokumentacja powykonawcza** |
|  | Po zakończeniu realizacji, Zamawiający wymaga dostarczenia dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań minimum w formie elektronicznej. Dokumentacja powykonawcza musi zawierać minimum:   1. opis ogólnych informacji o rozwiązaniach; 2. opis architektury logicznej; 3. opis ról użytkowników, uprawnień użytkowników; 4. zestawienie loginów i haseł do rozwiązań; 5. zestawienie ustawień wszystkich rozwiązań; 6. instrukcje instalacji, konfiguracji, uruchomienia; 7. zestawienie licencji; 8. listę autoryzowanych kontaktów serwisowych; |

|  |  |
| --- | --- |
|  | ***Moduły dodatkowe, pożądane podlegające ocenie w kryterium „jakość”*** |
| **1** | **Ochrona aplikacji chmurowych** |
|  | Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Sharepoint oraz aplikację Teams. |
|  | Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365. |
|  | Administrator musi mieć możliwość wskazania, które konto użytkownika będzie  objęte ochroną. |
|  | Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z  dowolnego miejsca w sieci. |
|  | Rozwiązanie musi być dostępne w języku polskim. |
|  | Konsola administracyjna rozwiązania musi posiadać możliwość raportowania. |
|  | Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do  rozwiązania tenantów lub do poszczególnych grup i użytkowników. |
|  | Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o wykorzystanie do analizy mechanizmów chmurowych, tego samego producenta. |
|  | Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta. |
|  | Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. Oraz Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. |
| **2** | **Zarządzanie podatnościami i aktualizacjami** |
|  | Wykrywanie podatności w systemach operacyjnych co najmniej Windows 10, Windows 11 oraz aplikacjach zainstalowanych na zarządzanych stacjach. |
|  | Baza wykrywanych podatności musi zawierać minimum 35000 CVE. |
|  | Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie. |
|  | Możliwość wyświetlania szczegółów danej podatności zawierające minimum nazwę aplikacji lub systemu operacyjnego, punktacje CVSS, opis wykrytej podatności, wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta. |
|  | Możliwość wykonania automatycznej aktualizacji dla minimum 150 popularnych aplikacji. |
|  | Możliwość tworzenia białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. |
|  | Możliwość stworzenia czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. |
|  | Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach. |
|  | Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania. |
|  | Możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami w konsoli centralnego zarządzania oraz wyłączenie powiadomień dla wybranej podatności |
| **3** | **Uwierzytelnianie wieloetapowe** |
|  | Musi wspierać systemy operacyjne minimum Microsoft Windows Server: Windows Server 2019 / Windows Server 2022. |
|  | Musi wspierać system operacyjne minimum Windows 10 / Windows 11. |
|  | Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. |
|  | Musi wspierać integrację minimum z: Microsoft Remote Desktop Web Access, Microsoft Terminal Services Web Access, Microsoft Remote Web Access. |
|  | Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS. |
|  | Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych, minimum: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej). |
|  | Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji. |
|  | Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN. |
|  | Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS. |
|  | Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego. |