

## OPIS PRZEDMIOTU ZAMÓWIENIA

**„DOSTAWA OPROGRAMOWANIA INFORMATYCZNEGO – ROZBUDOWA SYSTEMU OCHRONY URZĄDZEŃ ”**  
**Część 1 zamówienia na „Dostawę oprogramowania informatycznego” będącego częścią projektu pn. „Cyberbezpieczna Gmina Porąbka”**

L.P.	WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE
<b>I.</b>	<b>Rozbudowa systemu ochrony urządzeń</b>
<b>1</b>	<b>INFORMACJE OGÓLNE</b>
1)	Producent / Nazwa
2)	Istniejący system ochrony urządzeń ESET należy rozbudować w zakresie modułu posiadającego narzędzia wykrywania incydentów i automatycznego reagowania umożliwiającego korelację zdarzeń (XDR), mechanizmy uwierzytelniania wieloskładnikowego (MFA) oraz w zakresie proaktywnej ochrony przed zagrożeniami zero-day z analizą w odizolowanym chmurowym środowisku.
3)	W wyniku rozbudowy systemu o nowe moduły funkcjonalne przy zachowaniu dotychczasowej funkcjonalności 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 - 8
4)	Zamawiający dopuszcza wymianę istniejącego rozwiązania na rozwiązanie równoważne do istniejącego systemu ochrony urządzeń, realizującego minimum funkcjonalności opisane w pkt.2-8. 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 wyspecyfikowanego.
	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.
<b>2</b>	<b>WYMAGANIA OGÓLNE</b>
1)	Nowe moduły muszą być kompatybilne z istniejącym rozwiązaniem oraz muszą być zarządzane z jednej centralnej konsoli administracyjnej dostępnej z poziomu interfejsu WWW zabezpieczonego protokołem SSL.
2)	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.



3)	Moduł XDR musi być oparty o motor baz danych SQL celem zapewnienia maksymalnej wydajności pracy i maksymalnej ochrony danych. Motor bazy SQL należy dostarczyć wraz z modułem XDR.
4)	Wymagana ilość licencji na nowe moduły: minimum 105 szt.
<b>3</b>	<b>XDR</b>
1)	Automatyczna wizualizacja zdarzeń, incydentów i ataków ukierunkowanych
2)	Możliwość wyszukiwania zagrożeń na podstawie definiowanych filtrów
3)	Wbudowany zestaw reguł zapewniający reagowanie na wykryte incydenty z możliwością budowania własnych reguł oraz edycji istniejących.
4)	Możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
5)	Możliwość wprowadzania wykluczeń, po których nie zostanie wywołany alarm bezpieczeństwa
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)	Możliwość uruchomienia reguł w oparciu o dane historyczne.
9)	Możliwość blokowania plików po sumach kontrolnych.
10)	Możliwość ustawiania priorytetu zdarzeń.
11)	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.
12)	Możliwość oznaczenia plików DLL jako bezpieczne, pobrania do analizy oraz ich zablokowania.
13)	Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.
14)	Dla wykonanego skryptu lub pliku exe, weryfikacja powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15)	Możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
16)	Możliwość włączenia izolacji komputera od sieci.
<b>4</b>	<b>UWIERZYTELNIANIE WIELOSŁADNIKOWE (MFA)</b>
1)	Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
2)	Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemem operacyjnego.
3)	Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modułem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.
4)	Możliwość określenia metody uwierzytelniania dwusładnikowego użytkowników, minimum wiadomość SMS, aplikacja mobilna
5)	Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.



6)	Możliwość wysyłania wiadomości na telefony pracujące w roamingu.
7)	Możliwość wyboru użytkowników uwierzytelniania dwuskładnikowego.
8)	Możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.
9)	Rozwiązanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.
10)	W ramach modułu musi być zapewniony dostęp do dedykowanej aplikacji mobilnej działającej pod kontrolą Android i iOS
11)	Dostępne API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu minimum o usługę Active Directory. Dla środowisk nie wykorzystujących usług Active Directory musi być dostępny pakiet SDK umożliwiający implementację w tych środowiskach, dwuskładnikowego uwierzytelniania do autoryzacji użytkowników.
<b>5</b>	<b>SANDBOXING W CHMURZE</b>
1)	Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
2)	Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemem operacyjnym.
3)	Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modułem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.
4)	Ochrona przed zagrożeniami 0-day.
5)	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.
6)	Możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
7)	Możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
8)	Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
9)	Możliwość wyświetlenia listy plików, które zostały przesłane do analizy.
10)	Możliwość analizowania plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
<b>6</b>	<b>OCHRONA STACJI ROBOCZYCH</b>
1)	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
2)	Ochrona przed rootkitami oraz podłączeniem komputera do sieci botnet.
3)	Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
4)	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5)	Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6)	Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
7)	Umieszczenia na liście wykluczeń wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.



8)	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).
9)	Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
10)	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.
11)	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.
12)	Blokowanie nośników wymiennych, bądź grup urządzeń wraz z możliwością tworzenia reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
13)	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.
14)	Automatyczna, inkrementalna aktualizacja silnika detekcji.
15)	Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
16)	Skaner EFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17)	Zintegrowany moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.
18)	Zintegrowany moduł kontroli dostępu do stron internetowych.
19)	Możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
20)	Ochrona przed zagrożeniami 0-day.
<b>7</b>	<b>OCHRONA SERWERÓW</b>
1)	Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2)	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3)	Skanowania dysków sieciowych typu NAS.
4)	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.
5)	Automatyczna, inkrementalna aktualizacja silnika detekcji.
6)	Możliwość wykluczania ze skanowania procesów.
7)	Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
8)	System zapobiegania włamaniom działający na hoście (HIPS).
9)	Skanowanie magazynu Hyper-V.
10)	Skaner EFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.



11)	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.
12)	Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
13)	Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
14)	Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
15)	Możliwość uruchomienia lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
<b>8</b>	<b>OCHRONA URZĄDZEŃ MOBILNYCH</b>
1)	Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2)	Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
3)	Możliwość skonfigurowania zaufanej karty SIM.
4)	Wysyłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowanie urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS.
5)	Wyświetlenie listy zainstalowanych aplikacji.
6)	Blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
7)	Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
<b>II.</b>	<b>Wymagania dodatkowe</b>
<b>1</b>	<b>INSTALACJA</b>
1)	Zamawiający wymaga instalacji wszystkich dostarczonych systemów na urządzeniach wskazanych przez Zamawiającego na etapie realizacji.
<b>2</b>	<b>KONFIGURACJA</b>
<b>Rozbudowa systemu ochrony urządzeń</b>	
1)	W przypadku instalacji lokalnej Wykonawca zainstaluje na dostarczonym serwerze i skonfiguruje motor baz danych SQL w sposób zapewniający stabilną pracę rozwiązania. Jeżeli instalacja motoru baz danych będzie wymagała instalacji dodatkowych bibliotek programowych, należy je doinstalować.
2)	W zakresie XDR należy skonfigurować i zoptymalizować reguły reagowania na incydenty oraz przygotować polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem.
3)	W zakresie MFA uruchomić możliwość uwierzytelniania dwuskładnikowego przez użytkowników minimum z wykorzystaniem aplikacji mobilnej lub SMS.
4)	W przypadku rozwiązania równoważnego: a) przygotować pakiety instalacyjne i zainstalować system na wszystkich stacjach komputerowych; b) przygotować wymagane polityki dla organizacji i działu IT; c) skonfigurować polityki szyfrowania; d) uruchomić wszystkie moduły;



	<ul style="list-style-type: none"> <li>e) włączenie domyślnych reguł zgodnie z wytycznymi Zamawiającego określonymi na etapie realizacji;</li> <li>f) wykonać dokumentację zawierającą opis wszystkich modułów, punktów konfiguracji (wraz z rzutami ekranowymi, adresacjami, loginami wraz z hasłami, zalecenia wdrożeniowe;</li> <li>g) przeprowadzić minimum 4 godzin instruktarzu stanowiskowego dla administratorów Zamawiającego zapewniającego pełne zrozumienie administracyjnych, instalacji oprogramowania systemowego i narzędziowego, znajomości i umiejętności realizacji procedur, znajomości wytycznych polityk bezpieczeństwa, potwierdzonego protokołem z wykonania instruktarzu.</li> </ul>
<b>3</b>	<b>DOKUMENTACJA POWYKONAWCZA</b>
1)	<p>Po zakończeniu realizacji, Zamawiający wymaga dostarczenia pełnej dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań. Dokumentacja powykonawcza musi zawierać minimum:</p> <ul style="list-style-type: none"> <li>a) opis ogólnych informacji o rozwiązaniach;</li> <li>b) schematy połączeń urządzeń i ich adresacje;</li> <li>c) zestawienie loginów i haseł do rozwiązań;</li> <li>d) zestawienie ustawień wszystkich rozwiązań;</li> <li>e) instrukcje instalacji, konfiguracji, uruchomienia;</li> <li>f) zestawienie licencji;</li> <li>g) listę autoryzowanych kontaktów serwisowych;</li> </ul>



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA