Załącznik nr 1 do zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa oprogramowania typu EDR do monitorowania i gromadzenia danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych dla Urzędu Miasta i Gminy Police

w ramach Projektu „Cyberbezpieczna Gmina Police” dofinansowanego ze środków Unii Europejskiej w ramach konkursu grantowego „Cyberbezpieczny Samorząd” realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Główny kod CPV:
48761000-0 – Pakiety oprogramowania antywirusowego

SPIS TREŚCI

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

1. [WO] WYMAGANIA OGÓLNE

Zamówienie jest realizowane w ramach projektu „Cyberbezpieczna Gmina Police” (skrót CGP))” dofinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027; Priorytet II: Zaawansowane usługi cyfrowe; Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Przedmiot zamówienia obejmuje dostawę 180 licencji oprogramowania typu EDR do monitorowania i gromadzenia danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych(dalej: Oprogramowanie).
Oprogramowanie jest niezbędne do zapewnienia bezpieczeństwa i ochrony urządzeń oraz systemów informatycznych przed zainfekowaniem. Oprogramowanie będzie służyć do wykrywania i blokowania aktywności wirusów, trojanów, ransomware i innego złośliwego oprogramowania.
Obecnie Zamawiający posiada oprogramowanie ESET PROTECT Essential bez funkcjonalności EDR.

W ramach OPZ użyto następujących typów wymagalności parametrów funkcjonalnych:
- "MUSI BYĆ" - brak spełnienia wymagania może stanowić podstawę do odrzucenia oferty lub rozwiązania umowy,
- "PUNKTOWANE" - spełnienie wymagania stanowi podstawę do naliczenia dodatkowych punktów na etapie oceny ofert zgodnie z kryteriami określonymi w zapytaniu ofertowym..

Zamawiający informuje, że wszelkie wskazane w OPZ wymagania dotyczące niniejszego postępowania, w szczególności: normy, specyfikacje techniczne, nazwy własne, numery katalogowe, znaki towarowe, patenty lub pochodzenie, źródła lub szczególne procesy, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę, mają charakter przykładowy.
Zostały one przywołane jedynie w celu sprecyzowania parametrów i wymogów techniczno-użytkowych przedmiotu zamówienia, Zamawiający dopuszcza materiały, urządzenia i technologie równoważne. Wszelkie materiały, urządzenia i rozwiązania równoważne, muszą spełniać następujące wymagania i standardy w stosunku do oprogramowania, urządzenia i rozwiązania wskazanego jako przykładowy, tj. muszą być co najmniej:
1. tego samego charakteru użytkowego (tożsamość funkcji),
2. tej samej charakterystyki materiałowej (rodzaj i jakość materiałów),
3. tych samych parametrów technicznych (wytrzymałość, trwałość, itp);
4. tych samych parametrów bezpieczeństwa użytkowania;
oraz muszą być
5. kompatybilne z istniejącą infrastrukturą Zamawiającego,
6. spełniać te same funkcje,
7. posiadać stosowne dokumenty dopuszczające do stosowania certyfikaty, atesty i aprobaty techniczne.
Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia.

Zamówienie powinno zostać zrealizowane z uwzględnieniem wymagań funkcjonalnych opisanych w poniższych rozdziałach, które należy traktować jako minimalne parametry do rozwiązań równoważnych.

Lp.	ID	Nazwa wymagania	Wymagalność
1.1.	WO_001	Liczba licencji Oprogramowania: 180 szt.	MUSI BYĆ
1.2.	WO_002	Pakiety oprogramowania antywirusowego o kodzie CPV: 48761000-0.	MUSI BYĆ
1.3.	WO_003	Wykonawca zapewnia świadczenie usług wsparcia technicznego producenta oprogramowania: od dnia podpisania protokołu zdawczo-odbiorczego do minimum dnia 30 czerwca 2026 r.	MUSI BYĆ
1.4.	WO_004	Termin dostawy licencji do 30 dni od podpisania umowy lub w deklarowanym skróconym terminie dostaw zgodnie z formularzem ofertowym (20 pkt. w przypadku skrócenia do 10 dni, 10 pkt. w przypadku skrócenia do 20 dni)	PUNKTOWANE

2. [WAZ] WYMAGANIA DLA ADMINISTRACJI ZDALNEJ W CHMURZE DLA OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
2.1.	WAZ_001	Producent Oprogramowania udostępnia rozwiązanie w chmurze.	MUSI BYĆ
2.2.	WAZ_002	Oprogramowanie umożliwia dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.	MUSI BYĆ
2.3.	WAZ_003	Oprogramowanie jest zabezpieczone przy użyciu protokołu SSL.	MUSI BYĆ
2.4.	WAZ_004	Oprogramowanie posiada mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.	MUSI BYĆ
2.5.	WAZ_005	Oprogramowanie posiada możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.	MUSI BYĆ
2.6.	WAZ_006	Oprogramowanie posiada możliwość zarządzania urządzeniami mobilnymi.	MUSI BYĆ
2.7.	WAZ_007	Oprogramowanie posiada możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.	MUSI BYĆ
2.8.	WAZ_008	Oprogramowanie posiada możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: a) Politykami, b) Raportowaniem, c) Zarządzaniem licencjami, d) Zadaniami administracyjnymi. Każda z funkcji posiada możliwość wyboru uprawnienia: odczyt, użyj, zapisz, brak.	MUSI BYĆ
2.9.	WAZ_009	Oprogramowanie posiada co najmniej 80 szablonów raportów, przygotowanych przez Producenta Oprogramowania.	MUSI BYĆ
2.10.	WAZ_010	Oprogramowanie posiada możliwość tworzenia grup statycznych i dynamicznych komputerów.	MUSI BYĆ
2.11.	WAZ_011	Oprogramowanie posiada możliwość tworzenia grup dynamicznych, na podstawie szablonu określającego warunki, które klient spełnia, aby zostać umieszczonym w danej grupie. Warunki te obejmują co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersję systemu operacyjnego oraz podzespoły komputera.	MUSI BYĆ
2.12.	WAZ_012	Oprogramowanie posiada możliwość automatycznego uruchamiania zadań, przynajmniej z wyzwalaczami: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.	MUSI BYĆ

3. [WOSR] WYMAGANIA DLA OCHRONY STACJI ROBOCZYCH DLA OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
3.1.	WOSR_001	Oprogramowanie wspiera systemy operacyjne Windows 10 oraz Windows 11.	MUSI BYĆ
3.2.	WOSR_002	Oprogramowanie wspiera architekturę ARM64.	MUSI BYĆ
3.3.	WOSR_003	Oprogramowanie zapewnia wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	MUSI BYĆ
3.4.	WOSR_004	Oprogramowanie posiada wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.	MUSI BYĆ
3.5.	WOSR_005	Oprogramowanie zapewnia wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	MUSI BYĆ
3.6.	WOSR_006	Oprogramowanie zapewnia skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	MUSI BYĆ
3.7.	WOSR_007	Oprogramowanie zapewnia skanowanie całego dysku, wybranych katalogów lub pojedynczych plików na podstawie wyboru użytkownika lub według harmonogramu.	MUSI BYĆ
3.8.	WOSR_008	Oprogramowanie zapewnia skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	MUSI BYĆ
3.9.	WOSR_009	Oprogramowanie posiada możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej kontrolnej (SHA1) oraz lokalizacji pliku.	MUSI BYĆ
3.10.	WOSR_010	Oprogramowanie umożliwia integrację z Intel Threat Detection Technology.	MUSI BYĆ
3.11.	WOSR_011	Oprogramowanie zapewnia skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od klienta pocztowego).	MUSI BYĆ
3.12.	WOSR_012	Oprogramowanie zapewnia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	MUSI BYĆ
3.13.	WOSR_013	Oprogramowanie posiada wbudowane dwa niezależne moduły znajdowania rozwiązań (heurystyczne) wykorzystujące: a) Pasywne metody heurystyczne, b) Aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru jednej lub obydwu metod jednocześnie.	MUSI BYĆ
3.14.	WOSR_014	Oprogramowanie zapewnia blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: a) Pamięci masowych, b) Optycznych pamięci masowych, c) Pamięci masowych Firewire, d) Urządzeń do tworzenia obrazów, e) Drukarek USB, f) Urządzeń Bluetooth, g) Czytników kart inteligentnych, h) Modemów, i) Portów LPT/COM, j) Urządzeń przenośnych.	MUSI BYĆ
3.15.	WOSR_015	Oprogramowanie posiada funkcję blokowania nośników wymiennych, bądź grup urządzeń oraz umożliwia użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
3.16.	WOSR_016	Oprogramowanie posiada działający na hoście moduł HIPS, który posiada możliwość pracy w jednym z pięciu trybów: a) Automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b) Interaktywny, w którym rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c) Oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d) 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 samoczynnie przełącza się w tryb pracy oparty na regułach, e) Inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.	MUSI BYĆ
3.17.	WOSR_017	Oprogramowanie jest wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: a) zainstalowanych aplikacji, b) usług systemowych, c) informacji o systemie operacyjnym i sprzęcie, d) aktywnych procesów i połączeń sieciowych, e) harmonogramu systemu operacyjnego, f) pliku hosts, g) sterowników.	MUSI BYĆ
3.18.	WOSR_018	Funkcja Oprogramowania generująca cały raport posiada przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.	MUSI BYĆ
3.19.	WOSR_019	Oprogramowanie posiada automatyczną, inkrementacyjną aktualizację silnika detekcji.	MUSI BYĆ
3.20.	WOSR_020	Oprogramowanie posiada tylko jeden proces, który jest uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).	MUSI BYĆ
3.21.	WOSR_021	Oprogramowanie posiada funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	MUSI BYĆ
3.22.	WOSR_022	Oprogramowanie posiada ochronę antyspamową dla programu pocztowego Microsoft Outlook.	MUSI BYĆ
3.23.	WOSR_023	Zapora osobista Oprogramowania pracuje w jednym z czterech trybów: a) Automatyczny, który blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, b) Interaktywny, który pyta się o każde nowo nawiązywane połączenie, c) Oparty na regułach, który blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez Administratora, d) Uczenia się, który automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Tryb ten umożliwia Administratorowi konfigurowanie czasu działania trybu.	MUSI BYĆ
3.24.	WOSR_024	Oprogramowanie posiada moduł bezpiecznej przeglądarki internetowej.	MUSI BYĆ
3.25.	WOSR_025	Bezpieczna przeglądarka internetowa Oprogramowania automatycznie szyfruje wszelkie dane wprowadzane przez Użytkownika.	MUSI BYĆ
3.26.	WOSR_026	Praca w bezpiecznej przeglądarce internetowej Oprogramowania jest wyróżniona poprzez odpowiedni kolor ramki przeglądarki internetowej oraz informację na ramce przeglądarki internetowej.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
3.27.	WOSR_027	Oprogramowanie posiada zintegrowany moduł kontroli dostępu do stron internetowych.	MUSI BYĆ
3.28.	WOSR_028	Oprogramowanie posiada możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	MUSI BYĆ
3.29.	WOSR_029	Oprogramowanie zapewnia ochronę przed zagrożeniami wykorzystującymi luki, które są nieznane Producentowi Oprogramowania (0-day).	MUSI BYĆ
3.30.	WOSR_030	W przypadku stacji roboczych, Oprogramowanie posiada możliwość wstrzymania pobierania plików za pośrednictwem: a) Przeglądarek internetowych, b) Klientów poczty e-mail, c) Z nośników wymiennych, d) Wyodrębnionych z archiwum.	MUSI BYĆ

4. [WOS] WYMAGANIA DLA OCHRONY SERWERA DLA OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
4.1.	WOS_001	Oprogramowanie wspiera systemy systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.	MUSI BYĆ
4.2.	WOS_002	Oprogramowanie zapewnia ochronę przed: a) Wirusami, b) Trojanami, c) Robakami, d) Innymi zagrożeniami.	MUSI BYĆ
4.3.	WOS_003	Oprogramowanie zapewnienie wykrywania i usuwania niebezpiecznych aplikacji typu: a) Adware, b) Spyware, c) Dialer, d) Phishing, e) Narzędzi hakerskich, f) Backdoor.	MUSI BYĆ
4.4.	WOS_004	Oprogramowanie zapewnienie możliwości skanowania dysków sieciowych typu NAS.	MUSI BYĆ
4.5.	WOS_005	Oprogramowanie posiada wbudowane dwa niezależne moduły znajdowania rozwiązań (heurystyczne) wykorzystujące: a) Pasywne metody heurystyczne, b) Aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru jednej lub obydwu metod jednocześnie.	MUSI BYĆ
4.6.	WOS_006	Oprogramowanie wspiera automatyczną, inkrementacyjną aktualizację silnika detekcji.	MUSI BYĆ
4.7.	WOS_007	Oprogramowanie posiada możliwość wykluczania ze skanowania procesów.	MUSI BYĆ
4.8.	WOS_008	Oprogramowanie posiada możliwość określenia typu podejrzanych plików, jakie będą przesyłane do Producenta Oprogramowania, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.	MUSI BYĆ

5. [WDOS] WYMAGANIA DODATKOWE DLA OCHRONY SERWERA DLA OPROGRAMOWANIA

5.1. [OSW] OCHRONA SERWERÓW WINDOWS

Lp.	ID	Nazwa wymagania	Wymagalność
5.1.1.	OSW_001	Oprogramowanie posiada możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.	MUSI BYĆ
5.1.2.	OSW_002	Oprogramowanie posiada system zapobiegania włamaniom działający na hoście (HIPS).	MUSI BYĆ
5.1.3.	OSW_003	Oprogramowanie wspieranie skanowania magazynu Hyper-V.	MUSI BYĆ
5.1.4.	OSW_004	Oprogramowanie posiada funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	MUSI BYĆ
5.1.5.	OSW_005	Oprogramowanie zapewnia administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: a) Pamięci masowych, b) Optycznych pamięci masowych, c) Pamięci masowych Firewire, d) Urządzeń do tworzenia obrazów, e) Drukarek USB, f) Urządzeń Bluetooth, g) Czytników kart inteligentnych, h) Modemów, i) Portów LPT/COM, j) Urządzeń przenośnych.	MUSI BYĆ
5.1.6.	OSW_006	Oprogramowanie automatyczne wykrywa usługi zainstalowane na serwerze i tworzy dla nich odpowiednie wyjątki.	MUSI BYĆ
5.1.7.	OSW_007	Oprogramowanie posiada wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.	MUSI BYĆ
5.1.8.	OSW_008	Oprogramowanie zapewnia możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	MUSI BYĆ
5.1.9.	OSW_009	Oprogramowanie posiada ochronę przed programami wymuszającymi okup za pomocą dedykowanego modułu.	MUSI BYĆ

5.2. [OSL] OCHRONA SERWERÓW LINUX

Lp.	ID	Nazwa wymagania	Wymagalność
5.2.1.	OSL_001	Oprogramowanie pozwala na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.	MUSI BYĆ
5.2.2.	OSL_002	Lokalna konsola administracyjna Oprogramowania powinna działać bez potrzeby uruchamiania i instalowania dodatkowej usługi serwera Web.	MUSI BYĆ
5.2.3.	OSL_003	Oprogramowanie, do celów skanowania plików na macierzach NAS/SAN, wspiera rozwiązanie Dell EMC Isilon.	MUSI BYĆ
5.2.4.	OSL_004	Oprogramowanie działa w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność zapewnia podwyższony poziom stabilności. W przypadku awarii jednego z komponentów, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.	MUSI BYĆ

6. [WS] WYMAGANIA DLA SYSTEMU SZYFROWANIA DANYCH OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
6.1.	WS_001	Oprogramowanie wspiera instalację aplikacji klienckich w środowisku Microsoft Windows 10 i Microsoft Windows 11.	MUSI BYĆ
6.2.	WS_002	Oprogramowanie wspiera zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).	MUSI BYĆ
6.3.	WS_003	Oprogramowanie posiada autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny z możliwością całkowitego lub czasowego wyłączenia tego uwierzytelnienia.	MUSI BYĆ
6.4.	WS_004	Oprogramowanie umożliwia szyfrowanie danych tylko na komputach z UEFI.	MUSI BYĆ

7. [WOSM] WYMAGANIA DLA OCHRONY SYSTEMÓW MOBILNYCH OPARTYCH NA SYSTEMIE ANDROID DLA OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
7.1.	WOSM_001	Oprogramowanie zapewnia skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.	MUSI BYĆ
7.2.	WOSM_002	Oprogramowanie zapewnia co najmniej 2 poziomy skanowania: inteligentne i dokładne.	MUSI BYĆ
7.3.	WOSM_003	Oprogramowanie zapewnia automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).	MUSI BYĆ
7.4.	WOSM_004	Oprogramowanie posiada możliwość skonfigurowania zaufanej karty SIM.	MUSI BYĆ
7.5.	WOSM_005	Oprogramowanie zapewnia wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a) Usunięcie zawartości urządzenia, b) Przywrócenie urządzenie do ustawień fabrycznych, c) Zablokowania urządzenia, d) Uruchomienie sygnału dźwiękowego, e) Lokalizację GPS.	MUSI BYĆ
7.6.	WOSM_006	Oprogramowanie zapewnia Administratorowi podejrzenie listy zainstalowanych aplikacji.	MUSI BYĆ
7.7.	WOSM_007	Oprogramowanie posiada możliwość blokowania aplikacji w oparciu o: a) Nazwę aplikacji, b) Nazwę pakietu, c) Kategorię sklepu Google Play, d) Uprawnienia aplikacji, e) Pochodzenie aplikacji z nieznanego źródła.	MUSI BYĆ

8. [WSC] WYMAGANIA DLA SANDBOX W CHMURZE DLA OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
8.1.	WSC_001	Oprogramowanie zapewnia ochronę przed zagrożeniami wykorzystującymi luki w Oprogramowaniu, które są nieznane Producentowi Oprogramowania (0-day).	MUSI BYĆ
8.2.	WSC_002	Producent Oprogramowania do działania zapewnia chmurę.	MUSI BYĆ
8.3.	WSC_003	Oprogramowanie posiada możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym: a) Archiwa, b) Skrypty, c) Pliki wykonywalne, d) Możliwy spam, e) Dokumenty, f) Inne pliki typu .jar, .reg, .msi.	MUSI BYĆ
8.4.	WSC_004	Administrator ma możliwość zdefiniowania po jakim czasie przesłane pliki zastają usunięte z serwerów Producenta Oprogramowania.	MUSI BYĆ
8.5.	WSC_005	Administrator ma możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek do chmury.	MUSI BYĆ
8.6.	WSC_006	Oprogramowanie pozwala na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.	MUSI BYĆ
8.7.	WSC_007	Po zakończonej analizie pliku, Oprogramowanie przesyła wynik analizy do wszystkich wspieranych produktów.	MUSI BYĆ
8.8.	WSC_008	Administrator ma możliwość podejrzenia listy plików, które zostały przesłane do analizy.	MUSI BYĆ
8.9.	WSC_009	Oprogramowanie pozwala na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.	MUSI BYĆ
8.10.	WSC_010	Oprogramowanie powinno działać bez instalacji dodatkowego agenta na stacjach roboczych.	MUSI BYĆ
8.11.	WSC_011	Oprogramowanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub Administratora, za pomocą wspieranego produktu. Administrator ma możliwość podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.	MUSI BYĆ
8.12.	WSC_012	Oprogramowanie odpowiednio oznacza przeanalizowane pliki. Analiza pliku może zakończyć się wynikiem: a) Czysty, b) Podejrzany, c) Bardzo podejrzany, d) Szkodliwy.	MUSI BYĆ
8.13.	WSC_013	W przypadku stacji roboczych, Oprogramowanie posiada możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem: a) Przeglądarek internetowych, b) Klientów poczty e-mail, c) Z nośników wymiennych, d) Wyodrębnionych z archiwum.	MUSI BYĆ
8.14.	WSC_014	W przypadku serwerów pocztowych Oprogramowanie posiada możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.	MUSI BYĆ
8.15.	WSC_015	Wykryte zagrożenia są przenoszone w bezpieczny obszar kwarantanny, z której Administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

9. [WMX] WYMAGANIA DLA MODUŁU EDR DLA OPROGRAMOWANIA

Lp.	ID	Nazwa wymagania	Wymagalność
9.1.	WMX_001	Oprogramowanie umożliwia dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.	MUSI BYĆ
9.2.	WMX_002	Serwer administracyjny posiada możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego Producenta Oprogramowania.	MUSI BYĆ
9.3.	WMX_003	Interfejs Oprogramowania jest zabezpieczony za pośrednictwem protokołu SSL.	MUSI BYĆ
9.4.	WMX_004	Serwer administracyjny posiada możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.	MUSI BYĆ
9.5.	WMX_005	Wykluczenia dotyczą procesu lub procesu „rodzica”.	MUSI BYĆ
9.6.	WMX_006	Utworzenie wykluczenia automatycznie rozwiązuje alarmy, które pasują do utworzonego wykluczenia.	MUSI BYĆ
9.7.	WMX_007	Kryteria wykluczeń są konfigurowane w oparciu o przynajmniej: a) Nazwę procesu, b) Ścieżkę procesu, c) Wiersz polecenia, d) Wydawcę, e) Typ podpisu, f) SHA-1, g) Nazwę komputera, h) Grupę, i) Użytkownika.	MUSI BYĆ
9.8.	WMX_008	Serwer posiada ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator ma możliwość utworzenia własnych reguł oraz edycji reguł dodanych przez Producenta Oprogramowania.	MUSI BYĆ
9.9.	WMX_009	Serwer administracyjny oferuje możliwość blokowania plików na podstawie sum kontrolnych. W ramach blokady można dodać komentarz oraz skonfigurować wykonywaną czynność, po wykryciu pliku o danej sumie kontrolnej.	MUSI BYĆ
9.10.	WMX_010	Administrator może weryfikować uruchomione pliki wykonywalne na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: a) SHA-1, b) Typ podpisu, c) Wydawcę, d) Opis pliku, e) Wersję pliku, f) Nazwę firmy, g) Nazwę produktu, h) Wersję produktu, i) Oryginalną nazwę pliku, j) Rozmiar pliku, k) Reputację i popularność pliku.	MUSI BYĆ
9.11.	WMX_011	Administrator, w ramach plików wykonywalnych oraz plików DLL, posiada możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.	MUSI BYĆ
9.12.	WMX_012	Administrator może weryfikować uruchomione skrypty na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator ma możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.	MUSI BYĆ
9.13.	WMX_013	W ramach przeglądania wykonanego skryptu, Administrator posiada możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.	MUSI BYĆ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Lp.	ID	Nazwa wymagania	Wymagalność
9.14.	WMX_014	W ramach przeglądania wykonanego skryptu lub pliku exe, Administrator ma możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: a) Modyfikacji plików i rejestru, b) Zestawionych połączeń sieciowych, c) Utworzonych plików wykonywalnych.	MUSI BYĆ
9.15.	WMX_015	Serwer administracyjny oferuje możliwość przekierowania do konsoli zarządzającej Oprogramowania od tego samego dostawcy, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej Oprogramowania, Administrator ma 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.	MUSI BYĆ
9.16.	WMX_016	Konsola administracyjna ma możliwość tagowania obiektów.	MUSI BYĆ
9.17.	WMX_017	Konsola administracyjna umożliwia połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.	MUSI BYĆ

10. [WMO] WYMAGANIA DLA OCHRONY USŁUGI MICROSOFT 365

Lp.	ID	Nazwa wymagania	Wymagalność
10.1.	WMO_001	Oprogramowanie obejmuje ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.	MUSI BYĆ
10.2.	WMO_002	Oprogramowanie posiada możliwość dodania kilku tenantów usługi Micosoft 365.	MUSI BYĆ
10.3.	WMO_003	Administrator ma możliwość wskazania, które konto użytkownika będzie objęte ochroną.	MUSI BYĆ
10.4.	WMO_004	Oprogramowanie jest zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.	MUSI BYĆ
10.5.	WMO_005	Oprogramowanie jest dostępne w języku polskim.	MUSI BYĆ
10.6.	WMO_006	Konsola rozwiązania posiada możliwość raportowania co najmniej: a) użytkowników, otrzymujących najwięcej spamu, b) użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, c) użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, d) kont użytkowników, które mogę być podejrzane.	MUSI BYĆ
10.7.	WMO_007	Konsola rozwiązania posiada funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.	MUSI BYĆ
10.8.	WMO_008	Dzienniki Exchange Online posiadają funkcjonalność informowania co najmniej: a) jaka ilość wiadomości została przeskanowania, b) wynik skanowania poszczególnej wiadomości, c) czynność podjęta przez rozwiązanie.	MUSI BYĆ
10.9.	WMO_009	Dzienniki Onedrive posiadają funkcjonalność informowania co najmniej o: a) zagrożeniach, które zostały wykryte, b) na jakim koncie zostały wykryte, c) jakie zagrożenie zostało wykryte, d) podjętą czynność.	MUSI BYĆ
10.10.	WMO_010	Oprogramowanie posiada funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.	MUSI BYĆ
10.11.	WMO_011	Istnieje możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.	MUSI BYĆ
10.12.	WMO_012	Administrator posiada możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.	MUSI BYĆ
10.13.	WMO_013	Administrator posiada możliwość konfiguracji rozwiązania w oparciu o co najmniej: a) wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, b) wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online, c) dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.	MUSI BYĆ
10.14.	WMO_014	Oprogramowanie zapewnia funkcję ochrony przed zagrożeniami 0-day.	MUSI BYĆ
10.15.	WMO_015	Funkcja ochrony przed zagrożeniami 0-day wykorzystuje do działania chmurę producenta.	MUSI BYĆ
10.16.	WMO_016	Funkcja ochrony przed zagrożeniami 0-day posiada 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.	MUSI BYĆ

Lp.	ID	Nazwa wymagania	Wymagalność
10.17.	WMO_017	Administrator ma możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.	MUSI BYĆ
10.18.	WMO_018	Oprogramowanie posiada możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.	MUSI BYĆ

11. [MZPA] WYMAGANIA DLA MODUŁU ZARZĄDZANIA PODATNOŚCIAMI I AKTUALIZACJAMI

Lp.	ID	Nazwa wymagania	Wymagalność
11.1.	MZPA_001	Oprogramowanie posiada możliwość wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.	MUSI BYĆ
11.2.	MZPA_002	Baza wykrywanych podatności zawiera minimum 35000 CVE.	MUSI BYĆ
11.3.	MZPA_003	Oprogramowanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych.	MUSI BYĆ
11.4.	MZPA_004	Automatyczne wykrywanie podatności wykonuje się zgodnie z harmonogramem, nie częściej niż raz dziennie.	MUSI BYĆ
11.5.	MZPA_005	Moduł wykrywania podatności umożliwia wyświetlanie szczegółów danej podatności zawierające minimum: a) nazwę aplikacji lub systemu operacyjnego, b) punktacje CVSS, c) opis wykrytej podatności, d) wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.	MUSI BYĆ
11.6.	MZPA_006	Moduł wykrywania podatności wykrywa podatności w minimum 700 aplikacjach.	MUSI BYĆ
11.7.	MZPA_007	Moduł zarządzania aktualizacjami umożliwia wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.	MUSI BYĆ
11.8.	MZPA_008	Moduł zarządzania aktualizacjami umożliwia stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji jest możliwy z poziomu listy przygotowanej przez producenta rozwiązania.	MUSI BYĆ
11.9.	MZPA_009	Moduł zarządzania aktualizacjami umożliwia stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji jest możliwy z poziomu listy przygotowanej przez producenta rozwiązania.	MUSI BYĆ
11.10.	MZPA_010	Zarządzanie aktualizacjami aplikacji umożliwia ręczne wdrażanie poprawek na wybranych stacjach.	MUSI BYĆ
11.11.	MZPA_011	Moduł zarządzania aktualizacjami oraz wykrywania podatności jest zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.	MUSI BYĆ
11.12.	MZPA_012	Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami jest w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.	MUSI BYĆ
11.13.	MZPA_013	Administrator konsoli posiada możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.	MUSI BYĆ
11.14.	MZPA_014	Moduł wykrywania podatności umożliwia wyłączenie powiadomień dla wybranej podatności.	MUSI BYĆ

12. [WDU] WYMAGANIA DLA OCHRONY POPRZEZ DWUSKŁADNIKOWE UWIERZYTELNIANIE

Lp.	ID	Nazwa wymagania	Wymagalność
12.1.	WDU_001	Rozwiązanie wspiera systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.	MUSI BYĆ
12.2.	WDU_002	Rozwiązanie wspiera system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.	MUSI BYĆ
12.3.	WDU_003	Rozwiązanie wspiera architekturę 32 i 64-bitową systemu Windows.	MUSI BYĆ
12.4.	WDU_004	Oprogramowanie wspiera integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.	MUSI BYĆ
12.5.	WDU_005	Oprogramowanie wspiera integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.	MUSI BYĆ
12.6.	WDU_006	Oprogramowanie wspiera integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.	MUSI BYĆ
12.7.	WDU_007	Oprogramowanie wspiera integrację z Microsoft Remote Desktop Web Access.	MUSI BYĆ
12.8.	WDU_008	Oprogramowanie wspiera integrację z Microsoft Terminal Services Web Access.	MUSI BYĆ
12.9.	WDU_009	Oprogramowanie wspiera integrację z Microsoft Remote Web Access.	MUSI BYĆ
12.10.	WDU_010	Rozwiązanie posiada wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.	MUSI BYĆ
12.11.	WDU_011	Aplikacja mobilna wspiera telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).	MUSI BYĆ
12.12.	WDU_012	Aplikacja mobilna do generowania OTP (jednorazowego hasła) jest dostarczona przez producenta rozwiązania w ramach zakupionej licencji.	MUSI BYĆ
12.13.	WDU_013	Użytkownik posiada możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.	MUSI BYĆ
12.14.	WDU_014	Aplikacja do działania nie wymaga od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) odbywa się w trybie offline.	MUSI BYĆ
12.15.	WDU_015	Dwuskładnikowe uwierzytelnienie jest możliwe również przy użyciu jednorazowych haseł SMS.	MUSI BYĆ
12.16.	WDU_016	Aplikacja zainstalowana na urządzeniach mobilnych umożliwia generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.	MUSI BYĆ
12.17.	WDU_017	Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.	MUSI BYĆ