

ZAPROSZENIE SZACOWANIE WARTOŚCI ZAMÓWIENIA

W związku z zamiarem przeprowadzenia postępowania publicznego pn.: „*Dostawa oprogramowania informatycznego*” będącego częścią projektu „Cyberbezpieczna Gmina Porąbka” finansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, **Wójt Gminy Porąbka**, jako Zamawiający zwraca się z prośbą o przedstawienie **szacunkowej wyceny dostaw** zgodnie z poniższą specyfikacją. **Oferowane dostawy muszą być zgodne z minimalnymi wymaganiami określonymi poniżej.**

ZAKRES ZAMÓWIENIA OBEJMUJE DOSTAWY WRAZ Z WDROŻENIEM ROZWIĄZAŃ:

- | | |
|---|----------|
| 1) Rozbudowy systemu ochrony urządzeń | - 1 szt. |
| 2) Systemu inwentaryzacji oraz zarządzania siecią | - 1 szt. |
| 3) Skaneru podatności | - 1 szt. |
| 4) Systemu DLP | - 1 szt. |

Zamawiający informuje, że przedmiotowe Zaproszenie nie stanowi ofert w rozumieniu art. 66 KC ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 11 września 2024 r. – Prawo zamówień publicznych (tj. Dz. U. z 2024 r. poz. 1320); ma ono wyłącznie na celu rozeznanie cenowe rynku wśród wykonawców mogących zrealizować powyższe zamówienie oraz uzyskanie wiedzy na temat szacunkowych kosztów związanych z planowanym zamówieniem publicznym.

Zamawiający prosi o przekazanie informacji na Formularzu szacowania zamówienia stanowiącym załącznik do Zaproszenia w terminie do **08 listopada 2024 r.** za pośrednictwem poczty elektronicznej na adres: **anna.omasta@ug.porabka.pl**

Osobą uprawnioną do udzielania odpowiedzi na ewentualne pytania w zakresie przedmiotu szacowanych dostaw jest Główny Specjalista ds. Informatyki Piotr Wojtusiak tel. 510 258 304, e-mail: piotr.wojtusiak@ug.porabka.pl

WÓJT GMINY PORĄBKA
Paweł Zemanek

L.P.	WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE
I.	Rozbudowa systemu ochrony urządzeń
1	INFORMACJE OGÓLNE
1)	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.
2)	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
2	WYMAGANIA OGÓLNE
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 40 szt.
3	XDR
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 wyzwolony 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.
4	UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)
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)	Możliwość określenia metody uwierzytelniania dwuskładnikowego 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.
5	SANDBOXING W CHMURZE
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.
6	OCHRONA STACJI ROBOCZYCH

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 tworzenie 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 UEFI, 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.
7	OCHRONA SERWERÓW
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 UEFI, 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.
8	OCHRONA URZĄDZEŃ MOBILNYCH
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)	Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowania 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.
II.	<i>Skaner podatności</i>
1	WYMAGANIA OGÓLNE
1)	Rozwiązanie musi być dostępne minimum w wersji chmurowej (SaaS).
2)	Możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych, które muszą być udostępnione w postaci obrazu maszyny OVA lub dysku VHDX.
3)	Uwierzytelnianie użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS.
4)	Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.
5)	Możliwość zarządzania systemem przy użyciu interfejsu API.
6)	Rozwiązanie musi być dostarczone z 68 licencjami na stacje robocze
2	
1)	Nieograniczona liczba skanów i nieograniczona liczba zaplanowanych skanów oraz skanów na żądanie.
2)	Nieograniczonej liczby węzłów skanowania z nieograniczoną liczbą węzłów skanowania, które umożliwiają skanowanie różnych części sieci w tym samym czasie.

3)	Możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami.
4)	Usługa skanowania sieci musi obsługiwać IPv6.
5)	Możliwość dodawania nowych profili skanowania sieciowego.
6)	Możliwość importu predefiniowanych przez producenta profili skanowania sieciowego.
7)	Możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania.
8)	Możliwość uwzględnienia drukarek w procesie skanowania.
9)	Możliwość uwzględnienia martwych hostów w skanach.
10)	Możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania.
11)	Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux.
12)	Profil skanowania sieciowego musi posiadać możliwość wyboru intensywności skanowania.
13)	Profil skanowania sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania.
14)	Rozwiązanie musi posiadać co najmniej 80 tys. testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania.
15)	Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej Scanner appliance zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta (tylko w wersji chmurowej).
16)	Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem.
17)	Rozwiązanie musi posiadać możliwość pobrania raportu CSV z modułu skanowania sieciowego w celu wyświetlenia listy zadań skanowania.
18)	Urządzenia znalezione podczas zadania skanowania muszą zostać automatycznie dodane do listy urządzeń wraz z odpowiednimi znacznikami (tagami), przypisanymi na podstawie wykrytych portów usług oraz systemu operacyjnego.
3	MONITOROWANIE
1)	Rozwiązanie musi posiadać mechanizm weryfikacji listowania na czarnych listach serwerów pocztowych i stron internetowych.
2)	Możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami: nazwa zasobu, lista wykrytych podatności.
3)	Możliwość przeglądania i analizowania stanu podatności wraz z określeniem statusu wykrytej podatności (minimum: nowa/aktywna/naprawiona) sieci oraz aplikacji internetowych.
4)	Możliwość skanowania REST API.
5)	Tworzenie i utrzymywanie tagów (grup) statycznych i dynamicznych.
6)	Możliwość wprowadzania i importowania zasobów kategorii Network IP
4	ZARZĄDZANIE PODATNOŚCIAMI
1)	<p>Pulpit nawigacyjny udostępniający:</p> <ul style="list-style-type: none"> a) wyniki skanowania podatności sieci wg ważności wraz z możliwością prezentacji na wykresie słupkowym/kołowym; b) otwarte zgłoszenia według ważności wraz z możliwością prezentacji na wykresie słupkowym/kołowym; c) top 10 wyników skanowania sieci wraz z możliwością wyświetlania celu zasobu: wszystkich lub wybranych adresów IP / tagów; d) ostatnie skanowania; e) nadchodzące skanowania; f) ciągłe monitorowanie alertów z wyborem okresu: dzień/tydzień;

2)	Możliwość sortowania, grupowania i priorytetyzacji podatności, minimum wg. stanu, statusu (nowa/aktywna/naprawiona) i ważności podatności, typu zasobu,
3)	Możliwość filtrowania listy podatności według podatności lub aplikacji internetowych / hosta.
4)	Możliwość tworzenia raportów bezpośrednio z menedżera podatności poprzez wybranie jednej lub więcej podatności.
5)	Możliwość ciągłego lub czasowego ignorowania wybranych podatności z podaniem powodu ignorowania.
6)	Możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawienia profilu monitorowania zmian za pomocą powiadomień i alarmów.
7)	Możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych.
5	RAPORTOWANIE
1)	Wbudowane raporty dotyczące skanowanej sieci, w tym raporty zgodności minimum z Ustawą o ochronie danych osobowych oraz ISO 27001.
2)	Możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami: a) raport oparty na określonym czasie skanowania b) raport oparty na wszystkich bieżących informacjach o podatnościach c) raport trendów z historią podatności
3)	Możliwość filtrowania raportów.
III. System inwentaryzacji oraz zarządzania siecią	
1	WYMAGANIA OGÓLNE
1)	Rozwiązanie do monitorowania i inwentaryzacji sprzętu i oprogramowania zainstalowanego na stacjach komputerowych.
2)	Rozwiązanie musi zapewniać utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
3)	Rozwiązanie musi być posiadać polski oraz angielski interfejs językowy.
2	MONITORING SIECI, SPRZĘTU KOMPUTEROWEGO ORAZ UŻYTKOWNIKÓW
1)	Kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
2)	Monitorowanie musi obejmować minimum serwery, routery, przełączniki, firewalle/UTMy w zakresie wykrywania urządzeń, wizualizacji stanu urządzeń wraz z ich połączeniami na mapach sieci.
3)	Monitorowanie musi obejmować protokoły minimum TCP/IP, HTTP, HTTPS, POP3, SMTP, IMAP, MAPI, FTP.
4)	Monitoring urządzeń sieciowych w zakresie ruchu sieciowego, połączonych stacji roboczych i generowanego przez nie ruchu.
5)	Rozwiązanie musi zapewniać obsługę szyfrowania SSL/TLS
6)	Obsługa urządzeń SNMP
7)	Monitorowanie aktywności użytkowników pracujących na stacjach roboczych, minimum w zakresie uruchomionych procesów, listy odwiedzin stron www, transferu sieciowego oraz wydruków.
8)	Blokowanie stron internetowych poprzez możliwość zezwolenia lub blokowania całego ruchu WWW dla danej stacji roboczej.
9)	Blokowanie ruchu na wskazanych portach TCP/IP.
10)	Możliwość blokowania uruchamiania aplikacji zdefiniowanej przez administratora.
11)	Automatycznie gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych.
12)	Raporty i statystyki informujące administratora o stanie infrastruktury informatycznej.
13)	Informowanie administratora o zmianach konfiguracji stacji roboczej oraz o pojawieniu się nowego urządzenia w sieci.



14)	Automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera usług katalogowych Active Directory/OpenLDAP lub równoważnych), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
3	INWENTARYZACJA OPROGRAMOWANIA
1)	Automatyczna inwentaryzację zainstalowanego na komputerach oprogramowania.
2)	Globalny przegląd wszystkich programów zainstalowanych na komputerach.
3)	Weryfikacja legalności oprogramowania wraz z powiadamianiem o przekroczeniu liczby licencji.
4)	Tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
5)	Okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
6)	Musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
4	INWENTARYZACJA SPRZĘTU
1)	Możliwość okresowej, automatycznej inwentaryzacji parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
2)	Odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
3)	Odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
4)	Inwentaryzacja urządzeń na podstawie kodów kreskowych.
5)	Przechowywanie informacji dotyczących infrastruktury IT oraz automatyczna aktualizowania zgromadzonych informacji.
6)	Automatyczne gromadzenie informacji o sprzęcie w zakresie: <ul style="list-style-type: none"> – płyty głównej w zakresie model, producent, nr. seryjny, – CPU w zakresie nazwy, modelu, producenta, częstotliwości, – HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci, – RAM w zakresie wielkości pamięci, – karty sieciowej w zakresie model, adres IP, adres MAC,
7)	Możliwość definiowania typów i atrybutów elementów wyposażenia.
8)	Możliwość generowania zestawienia wszystkich środków trwałych.
9)	Możliwość tworzenia i drukowania kodów kreskowych i QR dla środków trwałych.
10)	Możliwość drukowania kartoteki sprzętowej stanowiska komputerowego.
IV.	System DLP
1	WYMAGANIA OGÓLNE
1)	Wsparcie instalacji w oparciu o bazę MS SQL.
2)	Praca w architekturze serwer, agent, klienta gdzie komunikacja serwera zarządzającego z klientem odbywa się tylko przy pomocy agenta.
3)	Serwer administracyjny musi umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych.
4)	Rozwiązanie musi być dostępne minimum w polskiej wersji językowej.
5)	Możliwość aktualizacji komponentów własnych.
6)	Automatyczne pobieranie aktualizacji definicji kategoryzowania stron internetowych oraz aplikacji. Musi być możliwość wyłączenia automatycznego pobierania.
7)	Wymuszenie komunikacji w czasie rzeczywistym dla wybranej stacji komputerowej w celu sprawdzania konfiguracji.

8)	Możliwość zablokowania/uruchomienia trybu awaryjnego na stacji końcowej
9)	Możliwość zdefiniowania portów dla ruchu pocztowego które mają być monitorowane przez oprogramowania zainstalowane na stacji końcowej.
10)	Możliwość ustawień powiadomień dla użytkownika końcowego w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP.
11)	Możliwość audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach.
12)	Filtrowanie poprzez podanie zakresu czasu.
13)	<p>Analiza lub tagowanie nowo powstałych plików wrażliwych w oparciu o minimum:</p> <ul style="list-style-type: none"> – aplikację z której zostały utworzone – lokalizację lokalną oraz sieciową – adres URL, z którego został pobrany plik – format pliku – zawartość pliku
14)	Analiza lub tagowania posiadanych plików wrażliwych w oparciu o minimum : lokalizację lokalną oraz sieciową, format pliku oraz zawartość pliku.
15)	<p>Możliwość powiadamiania użytkownika jeśli zidentyfikuje w wiadomości e-mail m.in.:</p> <ul style="list-style-type: none"> – numery Kart kredytowych – numer PESEL – numer polskiego dowodu osobistego – wyrażenia regularne – określone ciągi znaków – numer IBAN
16)	<p>Dla tagowanych plików możliwość utworzenia reguł w oparciu o czynności:</p> <ol style="list-style-type: none"> a) blokowania oraz zezwalania na zapisywanie, przenoszenie plików do lokalizacji na dyskach lokalnych lub konfiguracji określonych lokalizacji, do której będzie możliwość bądź nie będzie możliwości zapisu. b) blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń. c) zabezpieczenia możliwości drukowania, utworzenia białej oraz czarnej listy drukarek. d) blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji sieciowej oraz określenie białej oraz czarnej listy lokalizacji sieciowych. e) blokowania oraz zezwalania wysyłki plików za pośrednictwem klientów pocztowych oraz określenia białej oraz czarnej listy adresów e-mail oraz domen. f) blokowania oraz zezwalania na zapisywanie, przenoszenie plików na dyski zaszyfrowane w oparciu o lokalnie zaszyfrowane dyski oraz zewnętrzne zaszyfrowane dyski. g) blokowania oraz zezwalania na zapisywanie, przenoszenie plików do folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint). h) blokowania oraz zezwalania na zapisywanie, przenoszenie plików poprzez usługę pulpitu zdalnego i) blokowania oraz zezwalania na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty CD/DVD oraz wirtualnego drukowania plików. j) uruchomienia wybranego formatu pliku przez wskazaną przez administratora aplikację.
17)	Możliwość określenia stref urządzeń pamięci masowej,
18)	Możliwość globalnego zablokowania oraz zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint).

19)	Szyfrowanie dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika.
20)	Możliwość tworzenia kluczy szyfrujących które będą kompatybilne z funkcjonalnością BitLocker dla zapewnienia transparentności współdzielenia zaszyfrowanych nośników wymiennych.
21)	Możliwość globalnego zablokowania, zezwolenia, dostępu tylko do odczytu z korzystania z określonych urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
22)	Możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
23)	Możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych, w sytuacji jeżeli użytkownik zapomni hasła.
24)	Blokowanie stron internetowych w oparciu o kategorię stron oraz po podaniu adresu URL. Musi istnieć możliwość konfiguracji przekierowania z dowolnej strony która została zablokowana.
25)	Możliwość określenia stref urządzeń pamięci masowej,
2	RAPORTOWANIE
1)	Możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
2)	Możliwość raportowania reguł bezpieczeństwa w oparciu o incydenty na plikach chronionych, ogółu wykonanych operacji na plikach, podsumowania wszystkich incydentów bezpieczeństwa, akcji użytkowników na zabezpieczonych plikach, zablokowanych operacji na dyskach lokalnych, zewnętrznych, podsumowanie korzystania z urządzeń oraz ich typów.
3)	Możliwość utworzenia raportu w oparciu o użycie aplikacji, zablokowanych aplikacji, zablokowanych drukarek, podsumowanie drukowania, zablokowane strony internetowe, zablokowanych użytkowników, aktywność użytkowników na serwerze, alarmy, ustawień klienta, kopii bezpieczeństwa, zarządzania stacjami końcowymi, dezaktywacją licencji oraz zaawansowanego debugowania.
4)	Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
5)	Raporty muszą być generowane do pliku PDF, XLS po podaniu lokalizacji zapisywanego pliku, na wskazane adresy e-mail.
3	ADMINISTRACJA
1)	Synchronizacja użytkowników oraz stacji roboczych z usługą Active Directory.
2)	Możliwość zarządzania bazą danych poprzez określone zadania – kopii bazy danych, kopii oraz usunięcia bazy danych, usunięcia bazy danych, ustawieniach kopii bazy danych - dostępne z poziomu konsoli wraz z określeniem automatycznego powtarzania zadań: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
3)	Możliwość zdefiniowania przedziału czasowego dla kopii zapasowej bazy programu.
4)	Funkcje automatycznej kopii bazy danych programu DLP co 7, 14, 30 dni
5)	Tworzenie nowych/usuwanie/klonowanie kont administratorów w konsoli programu.
6)	Możliwość zmiany hasła oraz loginu innego administratora.
7)	Przypisywanie / odbieranie uprawnień do wybranych modułów programu.
8)	Możliwość logowania za pośrednictwem grup domenowych administratorów.
9)	Możliwość ustawienia godzin w których nie będą obowiązywały użytkownicy reguły kontroli aplikacji oraz stron internetowych. Godziny pracy muszą być ustalane dla poszczególnych dni tygodnia.

10)	Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane do chmur lub innych źródeł WWW.
11)	Określanie bezpiecznych stref oraz domen do których pliki mogą zostać przesłane.
12)	Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane na urządzenia zewnętrzne.
13)	Możliwość przygotowania pliku instalacyjnego agenta.
14)	Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
15)	Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
4	KONSOŁA ZDALNA
1)	Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
2)	Możliwość współdziałania z bazą danych MS SQL Server.
3)	Logowanie do konsoli webowej musi opierać się na wcześniej utworzonych kontach użytkowników w konsoli aplikacyjnej.
4)	Uprawnienia dostępu wybranych użytkowników do poszczególnych informacji na temat grup komputerów lub grupy użytkowników w konsoli webowej, muszą być ustalane z poziomu konsoli aplikacyjnej.
5)	<p>Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz użycia sprzętu które są podzielone na:</p> <p>a) Bezpieczeństwo danych:</p> <ul style="list-style-type: none"> – przegląd informacji o incydentach bezpieczeństwa. – przegląd danych przychodzących. – przegląd danych wychodzących. – przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików. – podłączane/odłączane urządzenia przenośne. <p>b) Produktywność:</p> <ul style="list-style-type: none"> – przegląd informacji na temat produktywności użytkowników. – aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. – trendy <p>c) Eksploatacja sprzętu:</p> <ul style="list-style-type: none"> – przegląd informacji na temat eksploatacji sprzętu komputerowego. – eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. – eksploatacja drukarek. – eksploatacji sieci.
6)	Możliwość dodania klucza licencji.
7)	Możliwość konfiguracji/zmiany domyślnego serwera SMTP.



8)	Weryfikacja wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
9)	Generowanie raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz użycia sprzętu. Raporty muszą być generowane dla wybranych grup komputerów/użytkowników w interwałach tygodniowych lub miesięcznych. Raporty będą przesyłane drogą e-mailową.
V.	<i>Wymagania dodatkowe</i>
1	INSTALACJA I KONFIGURACJA
1)	Zamawiający wymaga instalacji i konfiguracji wszystkich dostarczonych systemów na urządzeniach wskazanych przez Zamawiającego na etapie realizacji.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA