Przedmiotowe środki dowodowe dla:

**Zakup i wdrożenie oprogramowania zwiększającego poziom bezpieczeństwa Informatycznego,**

w ramach projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23 w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

**Część 1. Oprogramowania EDR z konsolą do zarządzania w chmurze**

|  |  |  |
| --- | --- | --- |
| Parametr | Spełnia | Nie spełnia |
| Konsola administratora w języku polskim |  |  |
| Konsola web pozwala na zdalne połączenie graficzne z graficznym pulpitem zdalnym bez tuneli VPN |  |  |
| Program antywirusowy posiada możliwość skanowania zasobów sieciowych |  |  |
| Program antywirusowy posiada moduł automatycznej piaskownicy |  |  |
| Oprogramowanie umożliwia monitorowanie (monitorowanie wydajności, aktywnych procesów, zdarzeń aktualizacji systemu) |  |  |
| Program antywirusowy posiada moduł antywirusowy chroniący w czasie rzeczywistym |  |  |
| Program antywirusowy ma możliwość importowania oraz eksportowania ustawień |  |  |
| Moduł EDR ma funkcję śledzenia zdarzeń systemowych i sieciowych urządzeń na których jest wdrożony |  |  |
| Polityka bezpieczeństwa jest edytowalna i ma możliwość wprowadzania samodzielnie zdefiniowanych reguł |  |  |
| Dostawca zapewni wdrożenie rozwiązania u Zamawiającego |  |  |
| Wsparcie techniczne dystrybutora rozwiązań w języku polskim świadczone przez Inżyniera z certyfikatem Expert zatrudnionego przez autoryzowanego partnera składającego ofertę |  |  |
| Podmiot świadczący wsparcie techniczne ma Certyfikat ISO27001 |  |  |

**Część 3. Systemu do zarządzania infrastrukturą IT i zasobami ludzkimi**

|  |  |  |
| --- | --- | --- |
| Parametr | Spełnia | Nie spełnia |
| Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania |  |  |
| Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji |  |  |
| Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy |  |  |
| Przypisywanie sprzętu do wybranej firmy |  |  |
| Odczytywanie indeksów wydajności poszczególnych komponentów komputera |  |  |
| Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany |  |  |
| Odczyt informacji o module TPM |  |  |
| Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta |  |  |
| Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu |  |  |
| Zdalne włączanie i wyłączenie komputerów |  |  |
| Wykonywanie zadań dla wszystkich komputerów |  |  |
| Grupowa zmiana atrybutów |  |  |
| Inwentaryzacja licencji |  |  |
| Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów |  |  |
| Śledzenie zmian w stanie zainstalowanego oprogramowania |  |  |
| Ewidencja zdarzeń przypisanych do użytkowników |  |  |
| Analiza aktywności użytkowników |  |  |
| Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników |  |  |
| Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.) |  |  |
| Moduł sygnalista- Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej |  |  |
| Moduł sygnalista- Usuwanie metadanych z załączników zgłoszeń |  |  |
| Moduł sygnalista- Podział interfejsu na publiczny oraz dla wewnętrzny |  |  |
| Blokada trybu incognito w przeglądarce Google Chrome |  |  |
| Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydentu |  |  |
| Zdalne zarządzanie procesami i rejestrem |  |  |