**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA  
OPROGRAMOWANIE DO ZARZĄDZANIA RUCHEM SIECIOWYM I KONTROLI POŁĄCZEŃ NA KOŃCÓWKACH LAN (EDR)**

**OPROGRAMOWANIE EDR – 75 LICENCJI (65 licencji stacji roboczych + 10 serwerowych)**

(na potwierdzenie, w ramach przedmiotowych środków dowodowych należy przedstawić kartę katalogową oferowanego rozwiązania)

Producent oferowanego oprogramowania: ...............................

Nazwa oferowanego oprogramowania: ...............................

|  |  |
| --- | --- |
| WYMAGANIA MINIMALNE | |
| Zarządzanie, monitorowanie i analiza ruchu na końcówkach w sieci LAN: | |
| Oprogramowanie zapewni monitorowanie i analizę ruchu na końcówkach działających w sieci LAN | Spełnia/nie spełnia\* |
| **Rozwiązanie zapewni Generowanie raportów:**  **Zarządczy Raport Ryzyk**  **Raport Podatności**  **Szczegółowy raport o incydentach**  **Raport o wykorzystaniu licencji -**  **Operacyjny raport wykonawczy - w celu monitorowania postawy i działania w zakresie bezpieczeństwa, a także informacji o incydentach.** | Spełnia/nie spełnia\* |
| Automatyczna Obrona Przed Ruchomymi Celami (AMTD) **– Oprogramowanie będzie wykorzystywać technologię Automatycznego Przemieszczania Celów (Automated Moving Target Defence) w celu ochrony zasobów informatycznych. AMTD działa poprzez dynamiczne modyfikowanie struktury i konfiguracji środowiska IT, co skutecznie zwiększa złożoność ataku dla cyberprzestępców. Dzięki częstym zmianom ustawień i konfiguracji, napastnicy napotykają na stale zmieniające się środowisko, co znacząco utrudnia przeprowadzenie udanego ataku. Wymagane jest, aby dostarczane Oprogramowanie stosowało:** | |
| randomizację pamięci**;** | Spełnia/nie spełnia\* |
| dynamiczne zmiany adresów IP; | Spełnia/nie spełnia\* |
| ukrywanie struktury aplikacji | Spełnia/nie spełnia\* |
| Ochrona Przed Atakami Bezplikowymi (Fileless Attacks) | |
| Oprogramowanie wykryje i zablokuje ataki, które nie wykorzystują tradycyjnych plików wykonywalnych, co pozwala im omijać klasyczne systemy bezpieczeństwa bazujące na sygnaturach. | Spełnia/nie spełnia\* |
| Oprogramowanie zapewni ochronę przed atakami typu fileless poprzez technologię, która nie wymaga wskaźników IoC (Indicators of Compromise) ani sygnatur | Spełnia/nie spełnia\* |
| Oprogramowanie zapewni skuteczność w przypadku nowych, niezidentyfikowanych zagrożeń. | Spełnia/nie spełnia\* |
| Oprogramowanie pozwoli na natychmiastowe zneutralizowanie ataków, takich jak shellcode injections**,** process hollowing  czy AMSI bypass, zanim staną się  realnym zagrożeniem dla systemów informatycznych | Spełnia/nie spełnia\* |
| Ochrona Pamięci i Przeciwdziałanie Eskalacji Uprawnień | |
| Oprogramowanie zapewni ochronę na poziomie pamięci operacyjnej, zapobiegając próbom  wstrzykiwania kodu i innym technikom wykorzystywanym do nieautoryzowanego przejęcia zasobów  systemowych. | Spełnia/nie spełnia\* |
| Oprogramowanie zapewni ochronę przed iniekcją kodu w pamięci, np. reflective injection i process hollowing, przez co zminimalizuje ryzyko wykonania złośliwego kodu. | Spełnia/nie spełnia\*\* |
| Oprogramowanie będzie przeciwdziałać eskalacji uprawnień poprzez blokowanie technik obejścia  kontroli UAC oraz prób uzyskania dostępu do krytycznych usług systemowych, takich jak LSA (Local  Security Authority). | Spełnia/nie spełnia\* |
| Wymagania dotyczące wydajności i efektywności: | |
| Minimalny Wpływ na Wydajność Systemu – Oprogramowanie będzie działało efektywnie bez nadmiernego zużycia zasobów, takich jak procesor (CPU) i pamięć RAM. | |
| Oprogramowanie nie spowolni zauważalnie, codziennych operacji biznesowych. | Spełnia/nie spełnia\* |
| Oprogramowanie  będzie miało zaimplementowane  mechanizmy, które mają minimalny  wpływ na wydajność systemu,  zapewniając tym samym  bezpieczeństwo bez kompromisów dla  operacyjności. | Spełnia/nie spełnia\* |
| Oprogramowanie musi mieć zaimplementowane mechanizmy optymalizacyjne pozwalające na działanie w sposób niemal niewidoczny dla użytkowników, zachowując pełną efektywność i responsywność systemu. | Spełnia/nie spełnia\* |
| Brak wymogu ciągłych aktualizacji sygnatur | Spełnia/nie spełnia\* |
| Oprogramowanie ma funkcjonować bez konieczności częstych aktualizacji sygnatur lub ciągłego połączenia z chmurą. | Spełnia/nie spełnia\* |
| Oprogramowanie dzięki technologii AMTD ma oferować ochronę przed zagrożeniami bez potrzeby opierania się na sygnaturach czy wskaźnikach kompromitacji, co pozwala na działanie nawet w warunkach ograniczonej łączności sieciowej. Jest to kluczowe zwłaszcza dla organizacji, które dysponują starszymi infrastrukturami lub systemami o ograniczonym dostępie do Internetu | Spełnia/nie spełnia\* |
| Oprogramowanie zapewni proaktywne podejście do obrony – eliminując zagrożenia zanim osiągną etap egzekucji. | Spełnia/nie spełnia\* |
| Minimalizacja Alertów Fałszywie Pozytywnych | Spełnia/nie spełnia\* |
| Oprogramowanie ma zapewnić wysokiej jakości alerty, redukując liczbę fałszywych pozytywnych alarmów, które stanowią istotne wyzwanie dla zespołów bezpieczeństwa | Spełnia/nie spełnia\* |
| Oprogramowanie może działać zarówno jako samodzielna warstwa ochronna, jak i jako uzupełnienie dla obecnych systemów, takich jak Microsoft Defender. | Spełnia/nie spełnia\* |
| **Wymagania dodatkowe:** | |
| Oprogramowanie musi działać na minimum 65 stacjach roboczych oraz minimum 10 maszynach serwerowych (w tym maszynach wirtualnych) w środowisku Windows | Spełnia/nie spełnia\* |
| Oprogramowanie musi posiadać interfejs minimum w języku polskim lub angielskim | Spełnia/nie spełnia\* |
| Oprogramowanie musi generować raporty minimum w języku polskim lub angielskim | Spełnia/nie spełnia\* |
| Okres licencjonowania musi wynosić minimum 12 miesięcy z możliwością odnowienia licencji przed upływem okresu licencjonowania | Spełnia/nie spełnia\* |
| Oprogramowanie musi oferować stałe wsparcie techniczne producenta minimum w języku polskim lub angielskim za pośrednictwem dedykowanego środka komunikacji elektronicznej oraz dostęp do aktualizacji producenta przez cały okres licencjonowania | Spełnia/nie spełnia\* |
| Wykonawca dostarczy wraz z oprogramowaniem instrukcję wdrożenia minimum w języku polskim lub angielskim | Spełnia/nie spełnia\* |
| **Wymagania dotyczące wdrożenia:** | |
| Rodzaj wdrożenia: ON-CLOUD lub ON-PREMISE | Spełnia/nie spełnia\* |

\*niepotrzebne skreślić

Cena netto zaoferowanego produktu (Oprogramowanie) – 75 licencji (65 licencji stacji roboczych + 10 serwerowych):

…………………………………………………………………………………………

Cena brutto zaoferowanego produktu (Oprogramowanie) – 75 licencji (65 licencji stacji roboczych + 10 serwerowych):

…………………………………………………………………………………………

..............................................................................

Podpis osoby - osób upoważnionych do składania

oświadczeń woli w imieniu wykonawcy