**Część III – Opis przedmiotu zamówienia**

**EDR – przedłużenie licencji – pakiet 840 licencji**

|  |  |
| --- | --- |
| **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na okres 12 miesięcy.  Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. 12 miesięczną gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).  Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.  Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.  Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych. |
| **Ochrona EDR** | System EDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.  Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.  Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.  Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:   * Microsoft Windows 10 * Microsoft Windows 11 * macOS version 14 "Sonoma" * macOS version 13 "Ventura" * macOS version 12 "Monterey" * macOS version 11 "Big Sur"   Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:   * Microsoft® Windows Server 2016 Standard * Microsoft® Windows Server 2016 Essentials * Microsoft® Windows Server 2016 Datacenter * Microsoft® Windows Server 2016 Core * Microsoft® Windows Server 2019 Standard * Microsoft® Windows Server 2019 Essentials * Microsoft® Windows Server 2019 Datacenter * Microsoft® Windows Server 2019 Core * Microsoft® Windows Server 2022 Standard * Microsoft® Windows Server 2022 Essentials * Microsoft® Windows Server 2022 Datacenter * Microsoft® Windows Server 2022 Core   Wspierane przeglądarki internetowe:   * Microsoft Edge * Mozilla Firefox * Google Chrome * Safari   Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:     * + Microsoft Windows Server 2016   + Microsoft Windows Server 2019   + Microsoft Windows Server 2022     Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:     * + Microsoft Edge   + Mozilla Firefox   + Google Chrome   + Safari   Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.   1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku. 2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory. 3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach. 5. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 6. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:    * dostęp do pliku;    * tworzenie nowego procesu;    * nawiązane połączenia sieciowe;    * wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;    * zawartość skryptów uruchamianych na monitorowanej stacji. 7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej. 8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy). 11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 12. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. 13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów. 14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym. 16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 17. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 18. Każda detekcja zawiera co najmniej następujące informacje:     * Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.     * Data i czas wystąpienia podejrzanych zdarzeń.     * Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.     * Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.     * Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.     * Poziom ryzyka, określający istotność danej detekcji.     * Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu). 19. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK). 20. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal). 21. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne. 22. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania. 23. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu. 24. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji. 25. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu. 26. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie. 27. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora. 28. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach. 29. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań. 30. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres. 31. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF. 32. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi. 33. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim. 34. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji. 35. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru. 36. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR. 37. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie. 38. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 39. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami. 40. Dodanie klucza licencyjnego skutkuje aktywowaniem zawartości zakładki obsługującej dany produkt w portalu zarządzającym. |
| **Certyfikaty i standardy** | * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/endpoint-protection-platforms>   minimalne wymaganie:  minimalna liczba referencji 65  minimalna ocena z referencji 4,6   * Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market <https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions>   minimalne wymaganie:  minimalna liczba referencji 17  minimalna ocena z referencji 4,4  system musi posiadać certyfikaty:   * OPSWAT (dla EDR na poziomie min. Platinium), * AVLAB +++ * AV Comperative Advance + * AV-TEST (ochrona w 2023 na poziomie min.6)   Producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 lub równoważne oraz ISO 27001 lub równoważne na usługi związane z cyberbezpieczeństwem - przedmiotowy środek dowodowy składany wraz z ofertą. |
| **Rozszerzone wsparcie serwisowe** | System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [**60**] miesięcy.  System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  • Wsparcie telefoniczne zespołu certyfikowanych inżynierów.  • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.  • Doradztwo w zakresie konfiguracji.  • Zdalne wsparcie techniczne.  • Pomoc w zakładaniu zgłoszeń serwisowych u producenta.  • Przygotowanie do zdalnej konfiguracji.  • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.  • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.  • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.  • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.  Dla zapewnienia wysokiego poziomu usług producent systemu lub autoryzowany podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważne oraz ISO 27001 lub równoważne w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem - przedmiotowy środek dowodowy składany wraz z ofertą.  Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.  Przedmiotowy środek dowodowy składany wraz z ofertą: Oświadczenie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). |