*Załącznik nr 2 – formularz ofertowy techniczny – część nr 4*

*Zakup specjalistycznego oprogramowania oraz sprzętu w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych w Szpitalu (sygnatura: ZP/2501/104/22)*

*Uwaga: Wykonawca zostaje zobowiązany do uzupełnienia kolumny „Oferowane parametry” o opis spełnienia wymaganych minimalnych parametrów technicznych. Zamawiający wymaga ponadto, aby* ***przedmiotowe środki dowodowe, złożone wraz z ofertą,*** *potwierdziły sporządzony przez wykonawcę opis.*

**4. System EDR**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry****(wymagany opis)** |
| 1. | Wymagania Ogólne | System EDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. Dostarczona licencja musi zapewniać 3 letnie wsparcie oraz działanie systemu dla min. 310 stacji roboczych i 30 serwerów.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 7 z dodatkiem SP1
* Microsoft Windows 8.1 (32-bit i 64-bit)
* Microsoft Windows 10
* Microsoft Windows 11
* MacOS 11 “Big Sur”
* MacOS 10.15 “Catalina”
* MacOS 10.14 “Mojave”

Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:* Microsoft® Windows Server 2008 R2
* Microsoft® Windows Server 2012
* Microsoft® Windows Server 2016
* Microsoft® Windows Server 2019
* Microsoft® Windows Server 2022

Wspierane przeglądarki internetowe:* Microsoft Edge
* Mozilla Firefox
* Google Chrome
* Safari

Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze. |  |
| 2. | Zarządzanie | 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. Maksymalna ilość wysyłanych danych przez agenta uruchomionego na stacji roboczej z systemami Windows nie przekracza 25MB na 24 godziny.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
11. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
12. 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.
13. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
14. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
15. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
16. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
17. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
18. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
19. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
20. 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).
21. 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).
22. 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).
23. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
24. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
25. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
26. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
27. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
28. Rozwiązanie monitoruje aplikacje uruchomione na stacjach roboczych i serwerach i oznacza aplikacje zidentyfikowane jako szkodliwe lub potencjalnie niebezpieczne dla użytkownika.
29. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
30. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
31. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
32. 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.
33. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
34. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
35. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
36. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
37. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
38. 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.
39. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
40. 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.
41. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
42. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
43. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
44. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
45. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
46. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
47. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
48. 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.
49. 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.
50. 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.
51. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
52. Maksymalna ilość wysyłanych danych przez agenta uruchomionego na stacji roboczej z systemami Windows nie przekracza 25MB na 24 godziny.
53. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
54. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
55. 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.
56. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
57. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
58. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
59. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
60. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
61. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
62. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
63. 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).
64. 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).
65. 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).
66. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
67. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
68. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
69. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
70. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
71. Rozwiązanie monitoruje aplikacje uruchomione na stacjach roboczych i serwerach i oznacza aplikacje zidentyfikowane jako szkodliwe lub potencjalnie niebezpieczne dla użytkownika.
72. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
73. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
74. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
75. 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.
76. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
77. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
78. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
79. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
80. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
81. 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.
82. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
83. 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.
84. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
85. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
86. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
 |  |
| 3 | Gwarancje i licencje | Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego.W ramach usług wynikających z udzielonej gwarancji jakości oraz technicznego Wykonawca zapewnia:1. udostępnienie poprawek do Oprogramowania Aplikacyjnego, w przypadku stwierdzenia przez Zamawiającego błędu Oprogramowania Aplikacyjnego:
2. w przypadku tzw. błędu krytycznego, tj. takiego, który uniemożliwia użytkowanie Oprogramowania Aplikacyjnego (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego:
	* + 1. reakcja Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego „błędu krytycznego”) 1 dzień roboczy;
			2. czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 3 dni roboczych od chwili rozpoczęcia czynności serwisowych;
			3. w przypadku wystąpienia „błędu krytycznego”, Wykonawca, po uzyskaniu od Zamawiającego zgody, może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem błędu krytycznego; w takim przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły;
3. w pozostałych przypadkach, określanych jako „błędy zwykłe” - błędy Oprogramowania Aplikacyjnego inne niż błędy krytyczne:
	* + 1. czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego błędu zwykłego) wynosi do 15 dni roboczych;
			2. czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 60 dni roboczych od chwili rozpoczęcia czynności serwisowych
 |  |

|  |  |
| --- | --- |
| miejscowość: |  |
| data: |  |

(podpis pieczątka imienna osoby upoważnionej

do składania oświadczeń woli w imieniu Wykonawcy)