**EZ/190/2022/ESŁ**

**Załącznik nr 2.2 do SWZ**

**Szczegółowy opis przedmiotu zamówienia (SOPZ)**

**Część 2**

**System wykrywania i reagowania na cyberzagrożenie typu EDR (Endpoint Detection and Response)**

**w punktach końcowych infrastruktury informatycznej Zamawiającego**

**wraz z niezbędnymi licencjami**

Zadanie obejmuje dostawę i wdrożenie funkcjonalności EDR w użytkowanym przez Zamawiającego systemie antywirusowym ESET PROTECT Entry ON-PREM, subskrypcja ważna do 2023-12-25 (dla 700 stanowisk) wraz z rozszerzeniem licencji systemu antywirusowego (z funkcjonalnością EDR) o dodatkowe 300 nowych stanowisk.

**Wymagania dla systemu wykrywania i reagowania na cyberzagrożenia:**

1. **Serwer administracyjny**
2. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 lub nowszych.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
6. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
7. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
8. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
9. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
10. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
11. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
12. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
13. Serwer musi posiadać minimum 900 wbudowanych reguł, których wystąpienie, wyzwala alarm bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
14. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
15. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
16. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
17. Administrator musi posiadać 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.
18. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
19. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
20. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
21. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
22. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
23. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator 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.
24. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
25. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
26. Konsola administracyjna musi mieć możliwość tagowania obiektów.
27. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
28. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
29. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
30. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.
31. **Agent**
32. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019.
33. Pełne wsparcie dla systemów macOS 10.12 i nowszych.
34. Pełne wsparcie dla systemów Linux RHEL 7.6+/RHEL 8/Ubuntu 18.04/Ubuntu 20.04
35. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
36. Agent musi współpracować z produktem antywirusowym tego samego producenta.
37. Agent nie może działać bez produktu antywirusowego tego samego producenta.
38. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta.
39. Połączenie agenta do serwera zarządzającego musi być szyfrowane.
40. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.
41. **Dostawa i wdrożenie**
42. Wykonanie instalacji i konfiguracji systemu na serwerze Zamawiającego
43. Wykonanie przykładowych instalacji na wskazanych stacjach roboczych Zamawiającego.
44. Przeprowadzenie instruktażu dla min. 2 administratorów wskazanych przez Zamawiającego w wymiarze co najmniej 6 godzin.