GK.ZP.271.21.2024 Załącznik nr 1 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Część 2 - oprogramowanie EDR z wdrożeniem**

**OPIS I MINIMALNE PARAMETRY**

**Zamawiający dopuszcza sprzęt o równoważnych, nie gorszych parametrach niż te przedstawione poniżej.**

**Oprogramowania EDR z wdrożeniem – 50 licencji.**

**Nowoczesny system ochrony** **antywirus nowej generacji, który wykorzystuje zaawansowane metody detekcji i  usuwania zagrożeń, w celu ochrony przed atakami cybernetycznymi. O**party na chmurze (SaaS) do ochrony punktów końcowych, które zapewnia zaawansowane funkcje wykrywania, zapobiegania, monitorowania i wyszukiwania różnego rodzaju wyrafinowanych zagrożeń oraz grup przestępczych. Oferujący zdalny wgląd do punktów końcowych w całym środowisku, umożliwiając natychmiastowy dostęp do informacji odnośnie ataku („kto, co, kiedy, gdzie i jak”). Spełniający wymagania:

1. System musi działać w architekturze klient - serwer.

2. Zarządzanie system musi być scentralizowane i dostępne przez stronę internetową.

3. Zarządzanie systemem musi odbywać się tylko poprzez jedną konsolę.

4. Połączenie klient - serwer musi być zabezpieczone protokołem TLS.

5. Klient instalowany na systemach końcowych musi obsługiwać co najmniej następujące

platformy systemowe:

Microsoft:

● Windows Server 2022

● Windows Server 2019

● Windows Server 2016

● Windows Server 2012 R2

● Windows Server 2012

● Windows 11 (22H2)

● Windows 11 (21H2)

● Windows 10 (22H2)

● Windows 10 (21H2)

● Windows 10 (21H1)

● Windows 10 (1809)

● Windows 7 SP1

Apple:

● macOS 14 (Sonoma)

● macOS 13 (Ventura)

● macOS 12 (Monterey)

Linux:

● Ubuntu 22.04 LTS

● Ubuntu 20.04 LTS

● Ubuntu 18.04 LTS

● SUSE Linux Enterprise Server 15.5 SLES 15 SP5

● SUSE Linux Enterprise Server 12.5

● Red Hat Enterprise Linux 9.3

● Red Hat/CentOS 8.5

● Red Hat/CentOS 8.4

● Red Hat/CentOS 8.3

6. Konsola administracji zdalnej, służąca zarządzaniu rozwiązaniem musi być rozwiązaniem chmurowym, niedopuszczalne jest rozwiązanie “on-premise” (lokalna instalacja systemu centralnej administracji)

7. Logowanie do konsoli administracyjnej musi odbywać się za pośrednictwem przeglądarki. Do logowania nie może być wykorzystywana konsola w postaci dedykowanej aplikacji, która wymaga dodatkowej instalacji. Logowanie musi być zabezpieczone dwuetapowym uwierzytelnianiem.

8. Konsola administracyjna musi umożliwiać zdefiniowanie konkretnych adresów IP, z których użytkownicy mogą się zalogować.

9. Konsola musi umożliwiać logowanie z wykorzystaniem Single Sign-On i powinna wspierać takich dostawców jak: AD FS (Active Directory Federation Services), Okta, PingFederate, PingOne, Azure Active Directory.

10. Ta sama konsola musi umożliwiać zarządzanie systemem NGAV (next-generation antivirus) jak i systemem XDR (extended detection and response) pochodzącymi od tego samego producenta. Niedopuszczalne jest rozwiązanie, które zawiera więcej niż jedną konsolę administracyjną.

11. Administrator musi mieć możliwość pobrania plików instalacyjnych agenta systemu bezpośrednio z poziomu konsoli zarządzającej.

12. Wdrożenie i aktualizacja oprogramowania nie może wymagać ponownego uruchomienia stacji końcowej.

13. System musi zawierać funkcję automatycznej aktualizacji agentów do wersji zalecanej przez producenta, z opcją wymuszenia przez administratora instalacji konkretnej jego wersji.

14. Ochrona musi być realizowana z wykorzystaniem sztucznej inteligencji.

15. System musi w swoim działaniu wykorzystywać proces uczenia maszynowego.

16. System musi reagować w czasie rzeczywistym na zagrożenia pojawiające się na stacji końcowej w sposób pełni automatyczny, bez udziału i decyzji użytkownika, w oparciu o sztuczną inteligencję.

17. System musi zapewniać ochronę przed szkodliwym oprogramowaniem bez wykorzystania mechanizmów opartych na sygnaturach.

18. System nie może w swoim działaniu od strony stacji końcowej wykorzystywać mechanizmów HIPS.

19. System musi wykorzystywać w wykrywaniu zagrożeń wskaźniki ataku IOA (Indicators of Attack).

20. System musi zapewniać ochronę również kiedy urządzenie końcowe nie ma połączenia z konsolą administracyjną.

21. System powinien umożliwiać ochronę przed złośliwym oprogramowaniem typu “zero-day”.

22. System centralnej administracji musi wspierać tworzenie konfigurowalnych stref umożliwiających przypisanie urządzeń i polityk bezpieczeństwa.

23. System musi posiadać możliwość wyłączenia powiadomień na stacjach końcowych.

24. System musi monitorować oprogramowanie układowe pod kątem podejrzanych obrazów.

25. System musi umożliwiać definiowanie niestandardowych reguł IOA w celu zapobiegania uruchomieniu aplikacji (np. PowerShell). Reguły muszą być definiowane co najmniej na podstawie nazwy procesu i ścieżki. Stworzone reguły mogą być blokowane lub monitorowane. Administrator podczas tworzenia musi mieć możliwość wskazania, jak istotna jest dla niego dana reguła w co najmniej 4 stopniach (np. informacyjna, niska, średnia, wysoka).

26. System musi umożliwiać definiowanie niestandardowych reguł, w których Administrator może zablokować lub monitorować daną aktywność na podstawie hashu, domeny, adresu IP.

27. Agent musi posiadać opcje, które mogą, ale nie muszą rejestrować produkt w Windows Security Center / Windows Defender Security Center.

28. Ochrona stacji końcowej musi być realizowana proaktywnie, a nie reaktywnie (tzn. przed wykonaniem kodu na stacji końcowej).

29. System musi posiadać mechanizm kontroli plików wykonywalnych.

30. System powinien posiadać mechanizm kontroli skryptów minimum takich jak: PowerShell, Python, makra pakietu Microsoft Office

31. System musi posiadać opcję automatycznego czyszczenia kwarantanny.

32. Konsola administracji zdalnej musi umożliwiać tworzenie grup, do których będą automatycznie przypisywane stacje na podstawie określonych wcześniej przez administratora warunków.

33. Warunki, jakie może określić administrator, by stacja trafiła do odpowiedniej grupy to co najmniej: zakres adresów IP, nazwa urządzenia, członek grupy, system operacyjny.

34. System musi umożliwiać nadawanie różnych uprawnień dla zalogowanego użytkownika, w tym co najmniej tworzyć konta typu administrator, tylko do odczytu, menedżer grup oraz użytkownik.

35. Rozwiązanie musi być wyposażone w moduł raportowania, a system raportowania musi umożliwiać automatyczne generowanie raportów według ustawień, które zdefiniuje Administrator.

36. System raportowania musi umożliwiać Administratorowi tworzenie harmonogramu do generowania raportów i musi umożliwiać automatyczne ich wysyłanie poprzez: wiadomość e-mail, wiadomość w usłudze internetowej Slack, powiadomień z wykorzystaniem webhook’ów oraz wiadomość w aplikacji Microsoft Teams. Automatyczne raporty muszą być wysyłane w formacie .PDF.

37. Administrator musi mieć możliwość określenia, jakie typy incydentów będą widocznie w tym co najmniej: informacyjne, o niskim priorytecie, o średnim priorytecie, o wysokim priorytecie.

38. Administrator musi mieć możliwość określenia zakresu czasu, z jakiego będą wyświetlane informacje dotyczące incydentów w tym co najmniej: z ostatnich 24 godzin, z ostatnich 7 dni, z ostatnich 30 dni.

39. Administrator musi mieć możliwość wglądu w szczegóły danego incydentu bezpośrednio z panelu administracyjnego.

40. Administrator musi mieć możliwość utworzenia wykluczenia bezpośrednio z poziomu detekcji.

41. System musi posiadać mechanizm izolacji urządzenia w celu zapewnienia bezpieczeństwa sieci lokalnej. Odizolowane urządzenie powinno komunikować się tylko i wyłącznie z konsolą administracyjną.

42. System musi umożliwiać tworzenie reguł, w których Administrator wskaże dodatkowe podsieci, z którymi odizolowane urządzenie może dodatkowo się komunikować.

43. System musi umożliwiać automatyczną izolację urządzenia w momencie wykrycia detekcji lub incydentu.

44. Administrator musi mieć możliwość przeszukiwania stacji końcowych, w ramach którego może uwzględnić co najmniej takie parametry jak: nazwy plików, MD5, SHA256, adresy IP.

45. Wyszukiwanie musi być możliwe dla konkretnej grupy lub wszystkich urządzeń objętych ochroną systemem XDR.

46. Wyniki wyszukiwania muszą być dostępne do wglądu z poziomu konsoli administracyjnej.

47. Administrator w momencie przeglądania detekcji musi mieć możliwość wykonania analizy, dostępnej w postaci graficznej.

48. Graficzny wynik analizy danego obiektu lub incydentu musi przedstawiać ścieżkę aktywności obiektu w systemie.

49. Informacje dotyczące analizy incydentu muszą zawierać minimum takie informacje jak: tworzenie plików, uruchomionych procesów, zmianach w rejestrze, połączenia sieciowe.

50. Administrator musi mieć możliwość uzyskania informacji dotyczących stacji końcowej w tym co najmniej: nazwy urządzenia, wersji zainstalowanego agenta, grupy, do jakiej dane urządzenie jest przypisane, adresu IP, statusu (online lub offline), kiedy ostatnio komunikował się z konsolą administracyjną, kiedy pierwszy raz połączył się z konsolą administracyjną, systemu operacyjnego, lokalnego adresu IP, adresu IP bramy domyślnej, publicznego adresu IP, MAC adresu, modelu, w jakim pracuje urządzenie (wirtualna maszyna lub fizyczna), ostatnio zalogowani użytkownicy.

51. System XDR musi pozwalać na kontrolę klienta poprzez zdalny wiersz poleceń. Uruchomienie zdalnego połączenia musi być dostępne na żądanie administratora z konsoli administracyjnej.

52. Konsola administracyjna przed połączeniem się z wykorzystaniem zdalnego wiersza poleceń musi uwierzytelnić Administratora drugim składnikiem uwierzytelnienia.

53. System musi umożliwiać pisanie własnych skryptów w powłoce bash, PowerShell, zsh, a następnie musi umożliwiać ich wysyłanie na stację końcową.

54. System musi zapewniać model dostępu oparty na rolach, a mianowicie: - rola administratora – zapewnia administracyjny dostęp do zarządzania wszystkimi modułami, komponentami i politykami systemu; - rola audytora – zapewnia przegląd ustawień systemu bez prawa wprowadzania zmian; - rola analityka – zapewnia przegląd i przetwarzanie zdarzeń, generowanie i przesyłanie raportów;

55. Odinstalowywanie agenta musi być zabezpieczone tokenem, który jest generowany z poziomu konsoli administracyjnej. Generowanie tokenu musi być odpowiednio monitorowane, a sam Administrator podczas generowania tokenu powinien mieć możliwość podania powodu, dla którego generuje token.

56. Konsola administracyjna musi umożliwiać wyświetlanie osi czasu, na której zostaną przedstawione co najmniej takie informacje jak: w jakim okresie czasu urządzenie końcowe posiadało status online oraz w jakim okresie czasu użytkownik był zalogowany.