Cyberbezpieczny Samorząd

Załącznik nr 4

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI I

1. Przedmiotem zamówienia jest zakup i dostawa licencji oprogramowania antywirusowego z systemem EDR (Endpoint Detection and Response) i XDR (Extended Detection and Response) dla Urzędu Miasta w Baborowie na okres 24 miesięcy**.**
2. W miejscach, gdzie w opisie wymagań technicznych - równoważnych wskazano znaki towarowe, patenty, pochodzenie, źródło czy szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, Zamawiający dopuszcza składanie ofert równoważnych. Za rozwiązanie „równoważne" uznany zostanie zaoferowany produkt, który spełni kryteria/parametry równoważności opisane przez Zamawiającego.
3. Wykonawca, który na etapie składania oferty, powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego.
4. Wymagany okres licencjonowania wynosi 24 miesiące od dnia zawarcia umowy (planowany termin zawarcia umowy luty 2024 roku)
5. Instruktaż dla administratorów zamawiającego:
    a. wykonawca przeprowadzi instruktaż omawiający wszystkie komponenty, który będzie dotyczył konfiguracji oraz administracji dostarczonego oprogramowania dla administratora Zamawiającego.
    b. Wykonawca zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej.
    c. Program Instruktażu powinien obejmować zagadnienia związane z czynnościami instalacyjnymi, konfiguracyjnymi i administracyjnymi wdrażanego systemu – minimum wdrożenie oprogramowania na 1 serwerze i 4 stacjach roboczych).
    d. Instruktaż musi być przeprowadzony w języku polskim.
    e. W instruktażu będzie uczestniczyć 1 osoba.
6. Minimalne parametry techniczno-jakościowe Przedmiotu zamówienia przedstawione zostały poniżej:

1. **Licencja na oprogramowanie antywirusowe na stacje robocze w tym ochrona 9 serwerów – 65 szt. Bitdefender GravityZone Business Security Enterprise z sondą XDR na okres 24 miesięcy** lub równoważny spełniający kryteria/parametry równoważności opisane przez Zamawiającego.

Opis wymagań technicznych:

Cyberbezpieczny Samorząd

Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana 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/sondy na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

System Operacyjny Windows:

Systemy Operacyjne Komputerów

Pełne wsparcie:

- Windows 11
- Windows 10

Systemy operacyjne serwera

Pełne wsparcie:

Windows Server 2022
Windows Server 2019

Ochrona środowisk wirtualnych (SVE)

Środowiska wspierane:

- Microsoft Hyper-V Server, 2019 or Windows Server 2019 (including Hyper-V Hypervisor)

Systemy Operacyjne Mac OS X

- macOS Sonoma (14.x)
- macOS Ventura (13.x)

I. Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".

9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość dodawania wykluczeń na podstawie
a. Plik
b. Folder
c. Rozszerzenie
d. Proces
e. Hash pliku
f. Hash certyfikatu
g. Nazwa zagrożenia
h. Wiersz poleceń
i. IP/maska
13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
20. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH
21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.

23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Praca programu musi być niezauważalna dla użytkownika.
29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
32. Możliwość odblokowania ustawień programu po wpisaniu hasła.
33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
40. Wbudowany IDS
41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.

43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
44. Możliwość tworzenia list sieci zaufanych.
45. Możliwość dezaktywacji funkcji zapory sieciowej.
46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa)
50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
52. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
    a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:
    -Ochrony przeglądarki internetowej
    -Sieć i poświadczenia
    -Błędna konfiguracja systemu operacyjnego
    System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.
    b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
    c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
    d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.
f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
a) Możliwość wymuszenia funkcji DEP systemu Windows
b) Możliwość wymuszenia relokacji modułów (ASLR)
54. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
-Wczesny dostęp
-Dostęp do poświadczeń
-Wykrycie
-Crimeware
55. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.
Formaty plików jakie mogą być odzyskane:
3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
a) Ukierunkowane ataki
b) Podejrzane pliki i ruch w sieci
c) Exploity
d) Ransomware
e) Grayware

57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego
58. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
    a) Tolerancyjny
    b) Normalny
    c) Agresywny

59. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku
    a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora
    b) Możliwość przesłania archiwum zabezpieczonego hasłem
    c) Możliwość przesłania adresu URL
    d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania
61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
63. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
64. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB
65. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.
66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).
67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem.

4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
6. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
7. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

Stacje robocze i serwery Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Konsola zdalnej administracji

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3. Możliwość integracji wielu domen Active Directory
4. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
9. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
10. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
11. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
12. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
13. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
14. Możliwość generowania raportu co godzinę.

15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
16. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
17. Możliwość dodania etykiety do stacji roboczej.
18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
19. Możliwość przechowywania kwarantanny maksymalnie 180 dni
20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
21. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
22. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
23. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[2]
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie
    -Zakres adresów IP/IP
    -Adres bramy
    -Adres serwera WINS
    -Adres serwera DNS
    -Połączenie DHCP sufiksów DNS
    -Punkt końcowy może rozwiązać hosta
    -Typ sieci
    -Nazwa hosta
27. Integracja z serwerem Syslog.
28. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238
29. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
30. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
31. Funkcja pojedynczego logowania – Single Sign-on (SSO).
32. Możliwość naprawy instalacji z poziomu konsoli.

33. Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:
    -Zarządzane punkty końcowe
    -Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS oraz fizyczne punkty końcowe i maszyny wirtualne
    -Pięć najczęściej blokowanych zagrożeń
    -Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
    -Status incydentów bezpieczeństwa które wystąpiły
    -Stan modułów punktów końcowych
    -Ocena ryzyka firmy
    -Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
    -Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

34. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Pakiety
    b) Sieć
    c) Kwarantanna
    d) Licencjonowanie
    e) Integracje
    f) Polityki
    g) Raporty
    h) Konta
    i) Firmy
35. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane
36. Możliwość określenia własnego serwera NTP.
37. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
38. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.

39. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
40. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.
41. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
42. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
43. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
44. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
45. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
46. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
47. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, MacOS.
48. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
49. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
50. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
51. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
52. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.

II. EDR-Endpoint Detection and Response

Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze

Wspierane systemy operacyjne

A. Systemy desktopowe
- Windows 11
- Windows 10

B. Systemy operacyjne dla serwerów:
- Windows Server 2022
- Windows Server 2019

C. MacOS:
macOS Sonoma (14.x)
macOS Ventura (13.x)

Komponenty EDR

Główne elementy:
1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.

Wykrywanie podejrzanej aktywności

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
1. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
2. Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja
1. Produkt musi zapewniać wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
2. Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:

a) Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.

c) Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

Incydenty

Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

a) Filtrowania zdarzeń
b) Blokowania procesów
c) Dodawanie procesów do czarnej listy
d) Dodawanie procesów do białej listy
e) Izolacja hosta
f) Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)
g) Przesłanie pliku do Sandbox
h) Sprawdzenie informacji o pliku w Google
i) Sprawdzenie informacji o pliku w VirusTotal

Filtrowanie zdarzeń odbywa się na podstawie:

a) ID
b) Data utworzenia
c) Ostatnia aktualizacja
d) Status
e) Ocena zagrożenia od 10 do 100 punktów
f) Typ zdarzenia
   - W organizacji.
   - Na punkcie końcowym.

Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem.

Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.

Możliwość wyświetlenia zablokowanych hashy plików.

Możliwość dodania własnych hashy MD5 oraz SHA256

Możliwość importu hashy z pliku CSV

Możliwość filtrowania dodanych hashy na podstawie:

a) Typu hashu
b) Wartości hash
c) Źródło dodania
d) Informacje o źródle
e) Nazwa pliku
f) Firma której dotyczy wpis

g) Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.

Konsola Cloud – serwer administracyjny po stronie producenta

1. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).
2. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:

a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

-Ochrony przeglądarki internetowej
-Sieć i poświadczenia
-Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie.

3. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

a) Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.

b) Funkcja pojedynczego logowania – Single Sign-on (SSO).

c) Możliwość naprawy instalacji z poziomu konsoli.

d) Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

-Zarządzane punkty końcowe
-Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
-Pięć najczęściej blokowanych zagrożeń
-Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
-Status incydentów bezpieczeństwa które wystąpiły

-Stan modułów punktów końcowych
-Ocena ryzyka firmy
-Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.

4. Możliwość integracji sekcji Firmy z innymi systemami poprzez API.
5. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
6. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
7. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:

a) historia powłoki
b) wczytywanie bibliotek .dll z podejrzanej lokalizacji
c) Sesje logowania z użyciem jawnych danych uwierzytelniających
d) Elementy startowe Windows
e) Arp cache
f) Ip forwarding
g) Pobieranie listy wszystkie otwarte pliki dla każdego procesu w systemie docelowym.
h) Lista zamontowanych nośników
i) Filtry ip tables
j) Połączenia TLS które używają certyfikatów self-signed
k) Używane rozszerzenia w przeglądarce Chrome
l) Używane rozszerzenia w przeglądarce Firefox
m) Używane rozszerzenia w przeglądarce Safari
n) Źródła apt w systemach Linux
o) Wyświetlanie zainstalowanych pakietów DEB
p) Wyświetlanie zainstalowanych pakietów RPM
q) Pakiety Python zainstalowane w systemie
r) Lista zainstalowanych użytkowników którzy łączyli się z publicznych adresów IP
s) Lista użytkowników którzy zostali utworzeni w ciągu ostatnich 30 dni(Linux)
t) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS
u) Wykrywanie czy Kontrola Kont Użytkowników(UAC) jest wyłączona
v) Wykrywanie czy SecureBoot jest włączony

w) Lista zapamiętanych połączeń bezprzewodowych
x) Wykrywa, czy zmienił się domyślny folder startowy użytkownika
y) Wykrywa, czy zmienił się domyślny folder startowy maszyny

8. Filtrowanie zdarzeń odbywa się na podstawie:
   a) ID
   b) Data utworzenia
   c) Ostatnia aktualizacja
   d) Status
   e) Ocena zagrożenia od 10 do 100 punktów
   f) Typ zdarzenia
      - W organizacji.
      - Na punkcie końcowym.

III. XDR (Extended Detection and Response)

Komponent XDR powinien zapewniać rozszerzone wykrywanie, reagowanie i analiza informacji także w sieciach, serwerach, chmurze, SIEM i wielu innych. XDR przedstawia zdarzenia które miały wpływ na 2 bądź większą ilość punktów końcowych, np całą organizację.
System powinien działać w oparciu o sondę:
Sensor Network – system działa w oparciu o maszynę wirtualną importowaną do środowiska Hyper-V, która w trybie TAP otrzymuje kopię ruchu sieciowego po porcie SPAN. Zebrane metadane są następnie przesyłane do silnika korelacji zdarzeń. System musi posiadać następujące cechy:

1. Monitorować ruch sieciowy w poszukiwaniu oznak ataków
2. Ciągle nasłuchiwać ruchu sieciowego
3. Zbierać pakiety sieciowe ze wszystkich punktów końcowych w monitorowanych sieciach
4. Wykrywać wszystkie urządzenia komunikujące się sieciach IPv4 i IPv6, niezależnie od tego czy urządzenie jest zarządzane przez oprogramowanie antywirusowe.
5. Skanować ruch sieciowy urządzeń IoT
6. Wykrywać ruch pomiędzy systemami
7. Wykrywać próby eksfiltracji danych poza organizację
8. Wykrywać skanowanie portów
9. Wykrywać sieciowe ataki brute force