FS.271.1.2024

Załącznik nr 6 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

„Gmina Święciechowa cyberbezpiecznym samorządem – zakup licencji na oprogramowanie antywirus na okres 24 miesięcy”

1. Przedłużenie na okres 24 miesięcy licencji na oprogramowanie antywirusowe Bitdefender GravityZone Business Security Enterprise (Ultra) dla 61 użytkowników.

Zamawiający wymaga zachowania dotychczas użytkowanego identyfikatora i hasła do głównego klucza licencyjnego.

a) Dostarczone oprogramowanie musi być fabrycznie nowe i musi pochodzić z legalnego źródła.

b) Zamawiający wymaga minimum **24 miesięcznej gwarancji** producenta na dostarczone przez Wykonawcę oprogramowanie.

c) Oprogramowanie powinno posiadać min. 24 miesięczne wsparcie, obejmujące dostarczenie aktualizacji, zdalnie (telefon, e-mail, WW) wsparcie techniczne w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania – nie mniej niż 20 godzin w ciągu roku.

2. **Miejsce dostawy:** Urząd Gminy Święciechowa, ul. Ułańska 4, 64 – 115 Święciechowa.

3. Przedmiot zamówienia jest realizowany w ramach projektu **„Gmina Święciechowa cyberbezpiecznym samorządem”**, współfinansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021 – 2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.

4. Zamawiający dopuszcza zaoferowanie produktu równoważnego. Oferowany antywirus powinien być kompatybilny z obecnie używanym systemem centralnego zarządzania z Bitdefender GracityZone Control Center. Oferowane oprogramowanie musi współpracować z aplikacjami posiadanymi przez Zamawiającego, bez konieczności wprowadzenia jakichkolwiek modyfikacji.
Wykonawca, który powołuje się na rozwiązania równoważne jest zobowiązany wykazać, że oferowane przez niego oprogramowanie równoważne spełnia wymagania określone przez Zamawiającego wskazane w SWZ i Opisie Przedmiotu Zamówienia. W tym celu Wykonawca zobowiązany jest dołączyć do oferty opis zawierający szczegółowe dane oferowanego oprogramowania, wskazując równoważność w stosunku do oprogramowania Bitdefender GravityZone Business Security Enterprise (Ultra).

Ponadto produkt równoważny to taki, który spełnia następujące wymagania:

<u>Ochrona antywirusowa i antyspyware</u>

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.

FS.271.1.2024

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.

FS.271.1.2024

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)
Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.
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
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|o
ds|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r
3d|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.

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. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony mają 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 niezmienionych 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 Direktory.
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.
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.

FS.271.1.2024

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. Możliwośc ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
30. Możliwość zablokowania konta w konsoli, xjeżeli 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, 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.
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. Integracja z vCenter Server.
38. Integracja z Xen Server.

FS.271.1.2024
39. Integracja z nutanix Prism Element.
40. Możliwość integracji z Amazon EC2.
41. Intergracja z Azure.
42. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
43. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.

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 zapewnia 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 Gogle
i) Sprawdzenie informacji o pliku w VirusTotal

Filtrowanie zdarzeń odbywa się na podstawie (Tylko konsola on-premise):

a) Ocena zagrożenia od 10 do 100 punktów
b) Data wykrycia
c) Status
d) ID
e) Nazwa punktu końcowego
f) Typ ataku
a) Ransomware
b) Potencjalnie niechciana aplikacja
c) Malware
d) Exploit
e) Fileless
f) Password stealer
g) Downloader
h) Inne
i) Zdefiniowane przez użytkownika