Skoki, dnia 21.03.2024

ROiSO.2601.8.2024

Prowadzący sprawę: Witold Bzdęga

it@gmina-skoki.pl

Tel.: 61 8 925 825

Segment B pok. nr: 7

# ZAPYTANIE O CENĘ

# w ramach projektu „Gmina Skoki cyberbezpiecznym samorządem”

W imieniu Gminy Skoki zapraszamy wszystkich solidnych wykonawców do składania ofert na dostawę przedłużenia/rozszerzenia obecnie posiadanej licencji Bitdefender GravityZone Elite 50 :

**Bitdefender GravityZone Business Security Enterprise 100 licencji na okres 24mc**

**Program antywirusowy musi spełniać wszystkie warunki:**

- CPV - 48761000-0 – Pakiety oprogramowania antywirusowego na 100 stanowisk dla jednostki samorządu terytorialnego jeśli występuje/przysługuje to wersja GOV;

- możliwość zwiększenia o nowe licencje (zakup nowego sprzętu etc.)

- licencja na 24 mc.

- w przypadku zaproponowania innego rozwiązania niż obecnie posiadane dostawca musi zaplanować/wliczyć w cenę dostawy lokalne wdrożenie w siedzibie zamawiającego, poprzez deinstalacje obecnego rozwiązania ze wszystkich serwerów i urządzeń końcowych, instalacje nowego oprogramowania wraz z konfiguracją środowiska (odwzorowania obecnej konfiguracji 1 do 1), wyjątków skanowania, filtracji aplikacji, filtracji portów na firewall w zależności od serwera i urządzenia końcowego, filtracji POP3 i SMTP, itp… w sposób nie blokujący ciągłości pracy Urzędu i świadczonych usług. Wdrożenie będzie odbywać się pod fizycznym nadzorem administratora systemów teleinformatycznych JST.

Obsługiwane systemy operacyjne komputerów

Pełne wsparcie:

* Windows 11 October 2023 Update (23h2)
* Windows 10 November 2022 Update (22H2)
* Windows 11 September 2022 Update (22H2)
* Windows 11 (initial release)
* Windows 10 November 2021 Update (21H2)
* Windows 10 May 2021 Update (21H1)
* Windows 10 October 2020 Update (20H2)
* Windows 10 May 2020 Update (20H1)
* Windows 10 May 2019 Update (19H1)
* Windows 10 October 2018 Update (Redstone 5)
* Windows 10 April 2018 Update (Redstone 4)
* Windows 10 Fall Creators Update (Redstone 3)
* Windows 10 Creators Update (Redstone 2)
* Windows 10 Anniversary Update (Redstone 1)
* Windows 10 November Update (Threshold 2)
* Windows 10 (initial release)
* Windows 8.1
* Windows 8
* Windows Server 2022 Core
* Windows Server 2022
* Windows Server 2019 Core
* Windows Server 2019
* Windows Server 2016
* Windows Server 2016 Core
* Windows Server 2012 R2
* Windows Server 2012
* Windows Small Business Server (SBS) 2011
* Windows Server 2008 R2
* Debian 9 - 4.9.0 32-bit/64-bit
* Debian 10 - 4.19 32-bit/64-bit
* Debian 11 - 5.10 32-bit/64-bit
* Debian 12 – 6.1.0 64-bit
* Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit
* Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 6 64-bit
* Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit
* macOS Sonoma (14.x)
* macOS Ventura (13.x)
* macOS Monterey (12.x)
* macOS Big Sur (11.x)
* macOS Catalina (10.15)
* macOS Mojave (10.14)

Ochrona środowisk wirtualnych (SVE)

1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej

2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:

a) OVA

b) XVA

c) VHD

d) VMDK

Środowiska wspierane:

• VMware vSphere and vCenter Server versions:

o version 6.5

o version 6.7, including update 1, update 2a and update 3

o version 7.0, including update 1, update 2, update 2b, update 2c and update 2d

o version 8.0, including update 1, update 2

• VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x

• VMware Workstation 11.x, 10.x, 9.x, 8.0.6

• VMware Player 7.x, 6.x, 5.x

• Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)

**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 6 godzin.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi mieć wbudowany skaner wyszukiwania rootkitów
13. Możliwość odblokowania ustawień programu po wpisaniu hasła
14. Możliwość uruchomienia zadania skanowania z niskim priorytetem
15. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

**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
13. Plik
14. Folder
15. Rozszerzenie
16. Proces
17. Hash pliku
18. Hash certyfikatu
19. Nazwa zagrożenia
20. IP/maska
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
22. 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).
23. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
25. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
26. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
27. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
28. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH
29. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
30. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
31. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
32. Praca programu musi być niezauważalna dla użytkownika.
33. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
34. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
35. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
36. Możliwość odblokowania ustawień programu po wpisaniu hasła.
37. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
38. 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).
39. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
40. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
41. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
42. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
43. Wbudowany IDS
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:
53. 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.

1. System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
2. 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.
3. System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
4. 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.
5. System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie
6. 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:
7. Możliwość wymuszenia funkcji DEP systemu Windows
8. Możliwość wymuszenia relokacji modułów (ASLR)

Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.

1. 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

1. 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.

1. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
2. Ukierunkowane ataki
3. Podejrzane pliki i ruch w sieci
4. Exploity
5. Ransomware
6. Grayware
7. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego
8. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:
9. Tolerancyjny
10. Normalny
11. Agresywny
12. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku
13. Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora
14. Możliwość przesłania archiwum zabezpieczonego hasłem
15. Możliwość przesłania adresu URL
16. W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
17. Wbudowany sandbox musi działać w trybie monitorowania i blokowania
18. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
19. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości, która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
20. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
21. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB
22. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.
23. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).
24. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń.
25. Oprogramowanie umożliwia uruchomienie opcjonalnych modułów/sensowrów XDR Identity AD oraz XDR Network.

**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

1. Integracja z serwerem Syslog.
2. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238
3. Możliwośc ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
4. Możliwość zablokowania konta w konsoli, xjeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
5. Funkcja pojedynczego logowania – Single Sign-on (SSO).
6. Możliwość naprawy instalacji z poziomu konsoli.
7. 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

1. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
2. Pakiety
3. Sieć
4. Kwarantanna
5. Licencjonowanie
6. Integracje
7. Polityki
8. Raporty
9. Konta
10. Firmy
11. 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
12. Możliwość określenia własnego serwera NTP.
13. Integracja z vCenter Server.
14. Integracja z Xen Server.
15. Integracja z nutanix Prism Element.
16. Możliwość integracji z Amazon EC2.
17. Intergracja z Azure.
18. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
19. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
20. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
21. Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
22. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
23. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
24. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
25. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
26. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
27. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
28. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
29. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
30. 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.
31. 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.

**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 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:
4. Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
5. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
6. 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:

1. Filtrowania zdarzeń
2. Blokowania procesów
3. Dodawanie procesów do czarnej listy
4. Dodawanie procesów do białej listy
5. Izolacja hosta
6. Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)
7. Przesłanie pliku do Sandbox
8. Sprawdzenie informacji o pliku w Google
9. Sprawdzenie informacji o pliku w VirusTotal

**Oferty proszę składać przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem https://platformazakupowa.pl/pn/umig\_skoki w PLN**

Zastrzegamy, że postępowanie może zakończyć się brakiem wyboru oferty w przypadku przekroczenia szacowanych środków.

Zapytanie ofertowe nie jest podstawą do żadnych roszczeń w stosunku do Gminy Skoki lub jednostek jej podlegających wynikających z podjęcia decyzji lub działań w procesie ofertowania przez Oferenta. Wydatki poniesione przez Oferenta w związku z przygotowaniem i odpowiedzią na zapytanie ofertowe nie są zwracane przez Gminę Skoki. Zastrzega sobie prawo do wycofania zapytania ofertowego w dowolnym czasie, akceptacja odpowiedzi Oferenta na zapytanie ofertowe nie stanowi żadnego zobowiązania w stosunku do potencjalnego Dostawcy dopóki nie zostanie podpisana umowa o współpracy.

**Zamawiający wymaga:**

- oferty niespełniające powyższej specyfikacji nie będą rozpatrywane,

- merytorycznego/technicznego wsparcia telefonicznego oraz e-mail przez okres trwania licencji w języku polskim.

- warunki płatności: płatność jednorazowa, **14** dni od otrzymania prawidłowo wystawionej faktury i zrealizowania przedmiotu zamówienia.

- termin dostawy: **7** dni od zamówienia;

- gwarancja: Certyfikat z numerem licencji;

- wersja w języku polskim (jeżeli występuje) z polskiego kanału dystrybucji.

**W przypadku pytań:**

**- kontakt: proszę o wpisaniu w pole “Mój komentarz do oferty” kontaktowego / służbowego numeru telefonu. Informujemy również, że jest to miejsce na informacje dodatkowe związane z ofertą.**

**-technicznych lub merytorycznych, proszę o kontakt za pośrednictwem przycisku w prawym, dolnym rogu formularza "Pytania do specyfikacji" lub pod nr tel. 618925825**

**- związanych z obsługą platformy, proszę o kontakt z Centrum Wsparcia Klienta platformy zakupowej Open Nexus pod nr 22 101 02 02, czynnym od poniedziałku do piątku w godzinach 8:00 do 17:00.**

**Oficjalnym potwierdzeniem chęci realizacji zamówienia przez Zamawiającego jest wysłanie zamówienia lub podpisanie umowy.**

**Kryterium wyboru oferty**

1.Cena 100%

Dane kontaktowe

**Gmina Skoki**

**ul. Wincentego Ciastowicza 11**

**62-085 Skoki**

**it@gmina-skoki.pl**

**Tel.: 61 8 925 825**