ZP/49/2023 Załącznik nr 1 do Zapytania ofertowego – OPIS PRZEDMIOTU ZAMÓWIENIA

System Antywirusowy obejmujący
- 180 PC
- 50 urządzeń z systemem android
- Szkolenie certyfikowane dwóch administratorów od strony zamawiającego
- okres trwania subskrypcji 36 miesięcy

Ochrona antywirusowa i antyspyware PC / Serwery

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:

68. obsługiwane systemy operacyjne:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1
- Windows 10 IoT Enterprise
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- RHEL 7.x - 3.10.0 (starting from build 957)
- RHEL 8.x - 4.18.0
- RHEL 9x - 5.14.0
- Oracle Linux 7.x (UEK +RHCK) - 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) - 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) – 5.15.0
- CentOS 7.x - 3.10.0 (starting from build 957)
- CentOS 8 Stream- 4.18.0
- CentOS 9 Stream- 5.14.0
- Fedora 31 – 36 - supported until it expires.
- AlmaLinux 8.x - 4.18.0
- AlmaLinux 9.x - 5.14.0
- Rocky Linux 8.x - 4.18.0
- Rocky Linux 9.x - 5.14.0
- CloudLinux 8.x - 4.18.0
- CloudLinux 7.x - 3.10
- Miracle 8.4 - 4.18.0
- Debian 9 - 4.9.0
- Debian 10 - 4.19

- Debian 11 - 5.10
- Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15
- Ubuntu 18.04.x - 5.0 / 5.3 / 5.4
- Ubuntu 20.04.x - 5.4
- Ubuntu 21.10.x - 5.13
- Ubuntu 22.04.x - 5.15
- PopOS 22.04.x – 6.2
- Pardus 21 – 5.10
- Mint 20.3 – 5.4.0
- Mint 21 – 5.15.0
- SLES 12 SP4 - 4.12.14-x
- SLES 12 SP5 - 4.12.14-x
- SLES 15 SP1 - 4.12.14-x
- SLES 15 SP2 - 5.3.18-x
- SLES 15 SP3 - 5.3.18-x
- SLES 15 SP4 – 5.14.21
- openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x
- AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x
- Amazon Linux v2 - 4.14.x / 4.19.x, 5.10
- Amazon Linux 2023 – 6.1.x
- Google COS - -4.19.112 / 5.4.49
- Milestones 77, 81, 85 - 4.19.112 / 5.4.49
- Azure Mariner 2 - 5.15

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:
    - version 6.5
    - version 6.7, including update 1, update 2a and update 3
    - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d
- 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
- Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2.

- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 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)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1

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 (initial)
- 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)

- Windows 8.1
- Windows 8
- Windows 7 SP1

B. Systemy operacyjne dla serwerów:

- 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

C. MacOS:

- macOS Monterey (12.x)
- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)

D. Linux

Oparte o RPM

RHEL 7.x - 3.10.0 (starting from build 957)

RHEL 8.x - 4.18.0

RHEL 9x - 5.14.0

Oracle Linux 7.x (UEK +RHCK) - 3.10.0-957 - 4.18.0

Oracle Linux 8.x (UEK +RHCK) - 3.10.0-957 - 4.18.0

Oracle Linux 8.x (UEK +RHCK) – 5.15.0

CentOS 7.x - 3.10.0 (starting from build 957)

CentOS 8 Stream- 4.18.0

CentOS 9 Stream- 5.14.0

Fedora 31 – 36 - supported until it expires.

AlmaLinux 8.x - 4.18.0

AlmaLinux 9.x - 5.14.0

Rocky Linux 8.x - 4.18.0

Rocky Linux 9.x - 5.14.0

CloudLinux 8.x - 4.18.0

CloudLinux 7.x - 3.10

Miracle 8.4 - 4.18.0

Oparte o Debian

Debian 9 - 4.9.0

Debian 10 - 4.19

Debian 11 - 5.10

Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15

Ubuntu 18.04.x - 5.0 / 5.3 / 5.4

Ubuntu 20.04.x - 5.4

Ubuntu 21.10.x - 5.13

Ubuntu 22.04.x - 5.15

PopOS 22.04.x – 6.2

Pardus 21 – 5.10

Mint 20.3 – 5.4.0

Mint 21 – 5.15.0

Oparte o SUSE

SLES 12 SP4 - 4.12.14-x

SLES 12 SP5 - 4.12.14-x

SLES 15 SP1 - 4.12.14-x

SLES 15 SP2 - 5.3.18-x

SLES 15 SP3 - 5.3.18-x

SLES 15 SP4 – 5.14.21

openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x

Cloud based Linux

AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x

Amazon Linux v2 - 4.14.x / 4.19.x, 5.10

Amazon Linux 2023 – 6.1.x

Google COS - -4.19.112 / 5.4.49

Milestones 77, 81, 85 - 4.19.112 / 5.4.49

Azure Mariner 2 - 5.15

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:

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. 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

Wyszukiwanie zdarzeń może odbywać się na podstawie:

a. Nazwa alertu
b. IP punktu końcowego
c. Hash MD5
d. Hash SHA256
e. Nazwa użytkownika

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.

6. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.

8. 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.

9. 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

System antywirusowy dla urządzeń z systemem Android

Rozwiązanie bezpieczeństwa dla urządzeń mobilnych musi zapewniać co najmniej następujące podstawowe funkcje:

1. Zaawansowane wykrywanie złośliwego oprogramowania.

2. Ochrona przed phishingiem - analizuje przychodzące wiadomości i wykrywa wszelkie złośliwe linki lub treści, które mogą zostać wykorzystane do pozyskania poufnych danych lub poświadczeń.

3. Bezpieczeństwo sieci - Zestaw narzędzi do ochrony urządzeń mobilnych przed różnymi zagrożeniami sieciowymi. Ta warstwa ochrony zapewnia bezpieczeństwo i integralność urządzeń mobilnych w obecnym krajobrazie zagrożeń

poprzez monitorowanie ruchu sieciowego, zapewnianie bezpiecznej łączności oraz wykrywanie i zapobieganie atakom.

4. Zgodność i egzekwowanie zasad - Ochrona urządzeń mobilnych przed różnymi zagrożeniami i zapewnienie, że są one używane bezpiecznie i zgodnie z przepisami, upewniając się, że wszystkie aplikacje są odpowiednio zweryfikowane.

5. Analiza zagrożeń mobilnych - zapewnia użytkownikom zabezpieczenia i analizy w czasie rzeczywistym

6. Integracja z rozwiązaniami do zarządzania urządzeniami mobilnymi (MDM) w celu zwiększenia bezpieczeństwa mobilnego (np. wymazanie urządzenia, blokada ekranu, w zależności od dostawcy MDM).

7. Filtrowanie treści internetowych - ostrzeganie i uniemożliwianie użytkownikom dostępu do potencjalnie szkodliwych witryn i linków, takich jak złośliwe oprogramowanie, phishing, botnety i podejrzane domeny lub witryny naruszające standardy organizacji.

8. Oprogramowanie musi mieć możliwość namierzenia lokalizacji urządzenia w momencie wystąpienia incydentu.

Rozwiązanie powinno obsługiwać integrację z następującymi dostawcami MDM:

- VMWare Workspace ONE UEM MDM

- BlackBerry Dynamics

- BlackBerry's UEM MDM (BES)

- Business Concierge MDM

- Citrix MDM

- MobileIron MDM

- SOTI MobiControl

Rozwiązanie powinno obsługiwać następujących dostawców SIEM:

- Splunk

- Azure Sentinel

- AT&T AlienVault

- Microsoft Defender ATP

- VMware Workspace ONE Intelligence

Rozwiązanie musi zapewniać funkcję pulpitu nawigacyjnego, która zapewnia widok zarządzania wszystkimi urządzeniami:

- Device Pool - wykres kołowy pokazujący rozkład urządzeń z aktywowaną i chronioną aplikacją, z oczekującymi statusami aktywacji.

- Urządzenia krytyczne - liczba urządzeń z jednym lub więcej zagrożeniami krytycznymi w ciągu ostatnich 90 dni.

- Ryzykowne urządzenia - wyświetlana jest liczba urządzeń z co najmniej jednym ryzykownym zdarzeniem w ciągu ostatnich 90 dni.

- Ryzyko systemu operacyjnego - pokazuje urządzenia z systemem Android i iOS, które są podatne na zagrożenia ze względu na przestarzałe i podatne na zagrożenia wersje systemu operacyjnego i muszą zostać zaktualizowane, aby wyeliminować to ryzyko.

- Bieżący wynik bezpieczeństwa - pokazuje ogólny wynik bezpieczeństwa na wszystkich urządzeniach w oparciu o ocenę aktywacji aplikacji Mobile Security, ryzyka i zagrożeń.

- Trend wyniku bezpieczeństwa - wyświetla wykres wyniku bezpieczeństwa wyświetlany w dziennym, tygodniowym lub miesięcznym przedziale czasowym.

- Kluczowe funkcje - wyświetla wartości stanu włączonych lub wyłączonych kluczowych funkcji rozwiązania.

- Top Critical Events - wyświetla pięć najważniejszych zagrożeń posortowanych na podstawie liczby zdarzeń z ostatnich 90 dni.

- Najbardziej ryzykowne zdarzenia - wyświetla pięć najbardziej ryzykownych zdarzeń posortowanych na podstawie liczby zdarzeń występujących w ciągu ostatnich 90 dni.

Rozwiązanie powinno wskazywać następujące poziomy statusów bezpieczeństwa:

- Krytyczny – Ten status wskazuje, że nastąpił rzeczywisty atak lub jest on w trakcie. Zazwyczaj oznacza to naruszenie bezpieczeństwa sieci i/lub urządzenia.

- Podwyższony - Ten poziom ważności oznacza zidentyfikowane ryzyko, które może prowadzić do ataku lub naruszenia bezpieczeństwa sieci lub urządzenia. Niekoniecznie oznacza to, że doszło do ataku.

- Niski - Ta informacja wskazuje na zdarzenie informacyjne (lukę w zabezpieczeniach).

- Normalny – Ten status wskazuje na normalne zdarzenie występujące w przypadku działań, takich jak zmiana DNS, zmiana proxy lub przekazanie sieci.

1. Rozwiązanie musi obsługiwać weryfikację aplikacji, z następującymi ocenami:

- Legalna/Złośliwa - aplikacja lub rozszerzenie jest oceniane na podstawie jej reputacji, autora i dostawców oprogramowania antywirusowego. Jeśli spełnia zalecany próg, jest oceniana jako złośliwa.

- Ryzyko dla prywatności - aplikacja lub rozszerzenie jest oceniane na podstawie zagrożeń dla prywatności, takich jak np. możliwość dostępu do kalendarzy, mikrofonów, lokalizacji.

- Ryzyko bezpieczeństwa - aplikacja jest oceniana na podstawie jej aspektów bezpieczeństwa/kodu w celu zidentyfikowania niebezpiecznych cech aplikacji.

2. Aplikacja może być oznaczona jako:

- Dozwolone

- Odmowa

- Niezgodność

- Brak lub nie dotyczy

1. Polityka wykrywania powinna być skonfigurowana zgodnie z najlepszymi praktykami, z następującymi krytycznymi wątkami domyślnie uwzględnionymi w polityce:

- Jailbreaking/ Rootowanie urządzenia

- Podniesienie uprawnień (EOP)

- MITM(Man-in-the-middle) - Przekierowanie ICMP

- MITM(Man-in-the-middle) - ARP

- Sabotaż systemu

- Nieuczciwy punkt dostępu

- MITM(Man-in-the-middle)

2. Administrator ma możliwość zmiany poziomów ważności zagrożeń:

- Krytyczny

- Podwyższony

- Niski

- Normalny

3. Akcje urządzenia możliwe do skonfigurowania w Polityce (w zależności od typu wątku):

a) Android:

- Odłącz Wi-Fi: Wyłączenie adaptera Wi-Fi i powrót do danych komórkowych, jeśli są włączone.

- Network Sinkhole: Akcja blokuje lub zezwala na zdefiniowane zakresy sieci/domen w oparciu o skonfigurowaną sieć IP/maskę i domeny.

- Wyłącz Bluetooth: Wyłącza adapter Bluetooth i rozłącza wszystkie bieżące połączenia Bluetooth.

- Tunnel Unsecured Traffic (Tuneluj niezabezpieczony ruch): Bezpieczny tunel VPN jest automatycznie inicjowany w celu obsługi ruchu przez niezabezpieczone połączenie.

b) iOS

- Włącz VPN: uruchamia zdefiniowaną sieć VPN w odpowiedzi na zagrożenie.

- Network Sinkhole: Akcja blokuje lub zezwala na zdefiniowane zakresy sieci/domen w oparciu o skonfigurowaną sieć/maskę IP i domeny.

- Wyłącz Bluetooth: Wyłącza adapter Bluetooth i rozłącza wszelkie bieżące połączenia Bluetooth.

- Tunnel Unsecured Traffic (Tuneluj niezabezpieczony ruch): Automatycznie inicjowany jest bezpieczny tunel VPN w celu obsługi ruchu przez niezabezpieczone połączenie.

c) Wykorzystanie Samsung Knox (możliwe działania):

- Wyłącz/odinstaluj/zablokuj aplikację: Usunięcie lub wyłączenie aplikacji z urządzenia.

- Odizoluj od sieci: Wyłączenie komunikacji sieciowej z aplikacjami, które są złośliwe, ale nie zostały jeszcze odinstalowane.

- Network Sinkhole: Blokuje lub zezwala na zdefiniowane zakresy sieci/domen w oparciu o skonfigurowaną sieć/maskę IP i domeny.

- Zapobieganie utracie danych: umożliwia wymazywanie danych z urządzenia (w tym z karty SD).

4. Administrator może oznaczyć aplikację jako:

- Dozwolona

- Odmowa

- niezgodna

- Brak lub nie dotyczy

1. Ustawienia polityki phishingu i zawartości muszą umożliwiać administratorowi ostrzeganie i ochronę użytkowników przed:

- Uzyskiwaniem dostępu do szkodliwych stron internetowych i linków.

- Uzyskiwaniem dostępu do stron internetowych i linków zawierających treści wymagające działania, takiego jak blokowanie, generowanie zagrożenia, ostrzeganie użytkownika lub kombinacja tych działań.

2. Filtrowanie treści.

Rozwiązanie musi obsługiwać dwie główne kategorie treści:

- Kategoria treści Security/Risk musi obejmować następujące podkategorie: Anonymizers, Botnets, Cryptocurrency Mining, Hacking, Illegal Software, Malware, Phishing, Spam, Suspected Domain, Jailbreak/Rooting Tools, Third-Party App Stores.

- Kategoria Treści dla dorosłych obejmuje następujące podkategorie: Treści dla dorosłych, Nagość, Pornografia, Edukacja seksualna, Stroje kąpielowe i odzież intymna.

Rozwiązanie musi przedstawiać kompleksowy wykaz wszystkich zidentyfikowanych zagrożeń dla systemów iOS i Android w systemie użytkownika, skategoryzowanych według systemu operacyjnego. Zawiera również odpowiednie CVE powiązane z każdym ryzykiem. Musi prezentować:

- Urządzenia z podanym systemem - wyświetla zagregowaną liczbę zagrożonych urządzeń. Dodatkowo, aby zapewnić podział liczby urządzeń z podatnymi wersjami systemu operacyjnego, z rozróżnieniem na systemy operacyjne iOS i Android.

- Urządzenia z możliwością aktualizacji - wyświetla łączną liczbę urządzeń, których dotyczy problem. Dodatkowo, aby zapewnić podział liczby na dwie kategorie: urządzenia z systemem iOS i urządzenia z systemem Android, które można zaktualizować.

- Urządzenia bez możliwości aktualizacji - wyświetla łączną liczbę urządzeń, których dotyczy problem. Dodatkowo, aby zapewnić podział liczby urządzeń z systemem iOS i Android, których nie można zaktualizować

Musi zawierać wraz z ogólną konfiguracją produktu także ustawienia konfiguracji prywatności:

- umożliwia administratorowi skonfigurowanie typu danych kryminalistycznych, które są gromadzone w przypadku wystąpienia zdarzenia dla każdej zdefiniowanej grupy konsoli (urządzeń).

- Co najmniej dostępny wybór szablonu z następującymi opcjami: Max, High, Medium, Low i Custom (gdzie Low to minimalna ilość danych wymagana do działania rozwiązania).