Prokuratoria Generalna
Rzeczypospolitej Polskiej

Urząd Prokuratorii Generalnej Rzeczypospolitej Polskiej
Biuro Budżetowo-Administracyjne
ul. Hoża 76/78, 00-682 Warszawa
tel. +48 22 392 31 09, fax +48 22 392 31 20
www.gov.pl/prokuratoria

KR-260- 4/24/ZBA

Warszawa, 16 lipca 2024 r.

12.07.2024 r. Wykonawca zwrócił się z prośbą o udzielenie odpowiedzi na poniższe pytania:

Pytanie nr 1

ad. pkt. 1.

Agent musi obsługiwać funkcjonalności Next Generation EPP (Endpoint Protection Platform) oraz EDR (Endpoint Detection and Response) w jednym autonomicznym agencie, który do realizacji swoich funkcjonalności nie potrzebuje łączności z chmurą lub konsolą zarządzającą. Wymagane jest wsparcie dla systemów operacyjnych Windows, macOS i Linux.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie obsługiwać funkcjonalności Next Generation EPP (Endpoint Protection Platform) oraz XDR (extended detection and response) nie potrzebuje łączności z chmurą lub konsolą zarządzającą. Funkcjonalność działa dla systemów operacyjnych Windows, macOS i Linux.

Odpowiedź: Zamawiający dopuszcza zaproponowane podejście, o ile inne wymagania Zamawiającego będą spełnione oraz funkcjonalności EPP i XDR będą realizowane w jednym autonomicznym agencie.

Pytanie nr 2

ad. pkt. 2.

Rozwiązanie musi być w stanie identyfikować zaawansowane zagrożenia, takie jak ataki bez plikowe, 0-day malware czy wykorzystywanie podatności posiadanego software/hardware bez korzystania z silników reputacji lub silników detekcji opartej o sygnatury. Przez silnik reputacyjny rozumiemy identyfikację zagrożeń z wykorzystaniem następujących elementów reputacji: adresy IP, DNS, URL, skróty/hashe. Rozwiązanie musi wykorzystywać statyczne oraz dynamiczne AI do identyfikacji zagrożeń, również tych które nie są wcześniej znane.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie w stanie identyfikować zaawansowane zagrożenia, takie jak ataki bez plikowe, 0-day malware czy wykorzystywanie podatności posiadanego software/hardware bez korzystania z silników reputacji lub silników detekcji opartej o sygnatury. Przez silnik reputacyjny rozumiemy identyfikację zagrożeń z wykorzystaniem następujących elementów reputacji: skróty/hashe. Rozwiązanie musi wykorzystywać statyczne oraz dynamiczne AI do identyfikacji zagrożeń, również tych które nie są wcześniej znane.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 3

ad. Pkt. 4. Ppkt. 5.

Funkcja Naprawy (Remediate): Zatrzymuje procesy, poddaje kwarantannie pliki binarne, usuwa połączone biblioteki, usuwa pliki źródłowe i przywraca konfigurację systemu operacyjnego, aplikacji i ustawień użytkownika do stanu sprzed rozpoczęcia ataku.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie miał funkcję Naprawy (Remediate): Zatrzymuje procesy, blokuje pliki, blokuje i usuwa pliki wykonywalne, izoluje komputer od sieci, skanuje komputer przed złośliwym oprogramowanie, wyłącza komputer

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 4

ad. Pkt. 4. Ppkt. 6.

Rollback: przywraca stan stacji końcowej do stanu z momentu utworzenia migawki VSS (Volume Shadow Copy), cofając zmiany wprowadzone przez złośliwy proces i skojarzone z nim zasoby. Agent powinien autonomicznie i w czasie zbliżonym do rzeczywistego przywrócić dane z chronionego hosta w przypadku ataku z wykorzystaniem szkodliwego oprogramowania typu ransomware .

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które w zamian będzie posiadał ponad 1300 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa, które również będą aktualizowane i dodawane nowe przez producenta. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 5

ad. Pkt. 6. Ppkt. 1

Przed wykonaniem (Pre-Execution): identyfikacja złośliwego oprogramowania na podstawie plików za pośrednictwem silnika reputacji. Funkcja nie wymaga aktualizacji baz danych sygnatur oraz aktualizacji plików sygnatur do realizacji swoich zadać. Dopuszcza się aby działanie tej funkcjonalności było zależne od chmury lub serwera zarządzającego – dlatego skanowanie całego dysku tym silnikiem powinno odbywać się TYLKO podczas początkowej instalacji i nie może być wymagane aby zapewnić poprawne działanie wszystkich funkcji bezpieczeństwa.

Odpowiedź: Wykonawca nie zadał żadnego pytania do tego punktu, zatem zapisy pozostają bez zmian.

Pytanie nr 6

ad. Pkt. 6. Ppkt. 2

Przed wykonaniem (Pre-Execution): rozwiązanie potrafi identyfikować nieznane szkodliwe oprogramowanie oparte na plikach na podstawie analizy statycznego z wykorzystaniem algorytmów uczenia maszynowego. Taka analiza musi odbywać się autonomicznie na stacji końcowej, bez zewnętrznych zależności lub zewnętrznego przetwarzania. Funkcjonalność nie może wymagać do działania uwzględnienia znanych IoC (DNS, IP, URL, HASH), a detekcja tego typu musi działać w czasie rzeczywistym podczas dostępu do systemu operacyjnego lub danego pliku.

Odpowiedź: Wykonawca nie zadał żadnego pytania do tego punktu, zatem zapisy pozostają bez zmian.

Pytanie nr 7

ad. Pkt. 6. Ppkt. 3

W czasie wykonywania (Run-Time): agent musi identyfikować i reagować na ataki z wykorzystaniem wyrafinowanych technik hackerskich (ataki bezplikowe, podatności i malware 0-day, złośliwe skrypt, lateral movement, oprogramowanie ransomware, trojany, APT itp.) Identyfikacja tych zagrożeń nie może wymagać zewnętrznych zależności, interwencji człowieka lub analizy danych poza chronioną stacją końcową. Funkcjonalność musi być realizowana w czasie zbliżonym do rzeczywistego poprzez wykorzystanie algorytmów sztucznej inteligencji. Znane IoC (DNS, IP, URL, HASH) nie mogą być wymagane jako środek identyfikacji zagrożenia

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które obsługuje następujące mechanizmy wykrywania złośliwego oprogramowania :

- *przed wykonaniem (Pre-Execution): identyfikacja złośliwego oprogramowania na podstawie plików za pośrednictwem silnika reputacji. Funkcja zaleca aktualizacji baz danych sygnatur oraz aktualizacji plików sygnatur do realizacji swoich zadań. Funkcja jest wymagana |do poprawnego działania modułu XDR.*
- *Przed wykonaniem (Pre-Execution): rozwiązanie potrafi identyfikować nieznane szkodliwe oprogramowanie oparte na plikach na podstawie analizy statycznego z wykorzystaniem algorytmów uczenia maszynowego. Analiza wykorzystuje połączoną moc sieci neuronowych (takich jak głębokie uczenie i pamięć krótkotrwała) oraz ręcznie wybraną grupę sześciu algorytmów klasyfikacyjnych, która pozwala wygenerować . Funkcjonalność obejmuje wykrywanie DNA, które używa modeli opartych na uczeniu maszynowym do skutecznej pracy z połączeniem z chmurą lub bez niego;*
- *W czasie wykonywania (Run-Time): agent identyfikuje i reaguje na ataki z wykorzystaniem wyrafinowanych technik hackerskich (ataki bezplikowe, podatności i malware 0-day, złośliwe skrypt, lateral movement, oprogramowanie ransomware, trojany, APT itp.) Identyfikacja tych zagrożeń nie musi wymagać zewnętrznych zależności, interwencji człowieka lub analizy danych poza chronioną stacją końcową. Funkcjonalność jest realizowana w czasie zbliżonym do rzeczywistego poprzez wykorzystanie algorytmów sztucznej inteligencji. Znane IoC (DNS, IP, URL, HASH) nie muszą być wymagane jako środek identyfikacji zagrożenia*

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 8

ad. Pkt. 7.

Rozwiązanie musi zapewniać silny mechanizm „Anti-Tamper", czyli mechanizmy ochrony przed manipulacja oprogramowaniem przez malware lub użytkownika końcowego. Taki mechanizm musi być chroniony unikalnym hasłem dla każdego komputera końcowego. Stan WŁ./WYŁ. Ochrony przed manipulacją powinien być opcją konfigurowalną w polityce bezpieczeństwa.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które posiada ochrone przed manipulacją oprogramowania przez malware lub użytkownika końcowego poprzez stosowania modułu HIPS - Host-based Intrusion Prevention System. System może być chroniony unikalnym hasłem przed wyłączeniem modułów.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 9

ad. Pkt. 9.

Rozwiązanie powinno zawierać otwarty interfejs API który umożliwia integracje z innymi rozwiązaniami, monitorowanie środowiska oraz automatyzacje niektórych z procesów. Dokumentacja interfejsuAPI powinna być natywnie dostępna z poziomu konsoli zarządzania Pytanie:
Czy zamawiający dopuszcza rozwiązanie, które posiada otwarty interfejs API który umożliwia integracje z innymi rozwiązaniami, monitorowanie środowiska oraz automatyzacje niektórych z procesów. Dokumentacja interfejsu API jest ogólnodostępna w dokumentacji producenta.

Odpowiedź: Zamawiający dopuszcza takie rozwiązanie.

Pytanie nr 10

ad. Pkt. 10.

Rozwiązanie musi obsługiwać architekturę typu Multi-Site lub Multi-Tenancy, aby całkowicie odseparować utworzone w systemie instancję i zapewnić odpowiedni dostęp administracyjny do konkretnej lokacji utworzonej zgodnie z modelem Multi-Site.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które obsługuje architekturę architekturę typu Multi-Site lub Multi-Tenancy, aby całkowicie odseparować utworzone w systemie instancję i zapewnić odpowiedni dostęp administracyjny do konkretnej lokacji utworzonej zgodnie z modelem Multi-Site. Rozwiązanie będzie obsługiwane przez jedną konsolę w chmurzę, którą można podzielić dla różnych lokacji oraz administratorów.

Odpowiedź: Zamawiający dopuszcza takie rozwiązanie.

Pytanie nr 11

ad. Pkt. 11

Rozwiązanie musi obsługiwać uwierzytelnianie SSO - SAMLv2. Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które wymaga użycia adres email oraz hasła do zalogowania się do Serwisu, dodatkowo umożliwia dodania dodatkowego mechanizmu bezpieczeństwa jak dwuskładnikowe uwierzytelnianie (2FA) poprzez aplikację mobilną, która generuje kod OTP.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie tzn. podtrzymuje konieczność obsługi uwierzytelniania SSO z wykorzystaniem SAMLv2.

Pytanie nr 12

ad. Pkt. 13

Rozwiązanie musi obsługiwać następujące formaty syslog: CEF, CEF2, RFC-5424, STIX i IOC.
Rozwiązanie powinno obsługiwać certyfikaty SSL i X.509 do szyfrowania i uwierzytelniania transportu syslog.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które obsługiwać następujące formaty syslog: CEF, JSON, LEEF v1. Rozwiązanie obsługuje komunikacje TLS do szyfrowania i uwierzytelniania transportu syslog.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 13

ad. Pkt. 15

Rozwiązanie musi umożliwiać zintegrowane z usługą Active Directory, aby możliwe było automatyczne przypisywanie agentów do grup, w celu powiązania ich z zasadami AD. Konsola zarządzania NIE powinna łączyć się z usługą Active Directory bezpośrednio za pośrednictwem programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi Device i User AD. Serwer zarządzania rozwiązaniem nie powinien mieć żadnych zależności od stanu usługi AD.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które umożliwiać zintegrowane z usługą Active Directory, aby możliwe było automatyczne przypisywanie agentów do grup, w celu powiązania ich z zasadami AD. Konsola zarządzania NIE powinna łączyć się z usługą Active Directory bezpośrednio za pośrednictwem programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi Device i User AD. Konsola zarządzająca podłączy się do skanera usług Active Directory, która będzie zainstalowana na systemie z dostępem do AD oraz będzie pobierała informację z AD, które przekaże do konsoli.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 14

ad. Pkt. 16

Rozwiązanie musi zawierać dashboard pokazujący wszystkie komputery, oraz możliwość ich filtrowania na podstawie atrybutów takich jak: OS, typ stacji końcowej, wersja agenta, występujące podatności, atrybuty AD, informacyjne telemetryczne, adresacja IP, charakterystyki hardware, ilości CPU, adresy Mac, interfejsy, nazwa hosta, nazwa grupy, domena). Lista powinna być dostępna do przeglądania w celu inwentaryzacji hostów, stosowania akcji dla podzbioru stacji końcowych lub mapowania stacji końcowych do grup. Musi zapewniać opcję wyświetlenia szczegółów stacji, takie jak aspekty telemetrii, stan stacji, aplikacje oraz zapewniać następujące opcje działania: Odłącz/ Połącz się od sieci (kwarantanna sieciowa, Uruchom ponownie OS, Zamknij system, Wyślij wiadomość do użytkownika, Odinstaluj agenta, Wyświetl zagrożenia.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które zawiera minimum 80 szablonów raportów, przygotowanych przez producenta oraz umożliwia tworzenia własnych raportów, które mogła pojawić się w dashboardzie. Natomiast z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania. Musi zapewniać opcję wyświetlenia szczegółów stacji, takie jak aspekty telemetrii, stan stacji, aplikacje oraz zapewniać następujące opcje działania: Odłącz/ Połącz się od sieci (kwarantanna sieciowa, Uruchom ponownie OS, Zamknij system, Wyślij wiadomość do użytkownika, Odinstaluj agenta, Wyświetl zagrożenia.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 15

ad. Pkt. 18

Rozwiązanie EPP / EDR musi mieć zapewniać funkcjonalność lokalnego firewalla dla chronionej stacji końcowej. Ochrona firewall musi umożliwiać realizację unikalnych polityk dla każdej chronionej grupy hostów. Reguły firewalla powinny umożliwiać uwzględnienie następujących parametrów: FQDN , IP, CIDR. Funkcjonalność musi być obsługiwana dla następujących systemów operacyjnych: Windows, Linux i MacOS.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które posiada autoryzacje stref i odbywa się min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. Natomiast podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. Funkcjonalność jest obsługiwana dla systemów operacyjnych Windows.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 16

ad. Pkt. 19

Rozwiązanie EPP / EDR musi mieć funkcjonalność kontroli urządzeń które próbują uzyskać dostęp do chronionej stacji. Kontrola urządzeń musi umożliwiać realizację unikalnych polityk dla każdej chronionej grupy hostów. Wymagana jest obsługa kontroli urządzeń dla następujących interfejsów: USB i Bluetooth.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które umożliwia administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.

Odpowiedź: Wymagania opisane w punkcie 19 są wymaganiami minimalnymi, zatem Zamawiający dopuści rozwiązanie spełniające dodatkowe funkcjonalności opisane z pytaniu.

Pytanie nr 17

ad. Pkt. 21

Przechowywanie danych EDR musi trwać co najmniej 14 dni w modelu opartym na chmurze SaaS.
Pytanie:
Czy zamawiający dopuszcza rozwiązanie EDR, które przechowuje dane co najmniej 7 dni w modelu opartym na chmurze SaaS .

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 18

ad. Pkt. 22

Funkcjonalność EDR musi mieć możliwość automatycznego i autonomicznego wykonywania wstępnego indeksowania i wstępnego korelowania zdarzeń, w momencie ich wystąpienia w chronionym środowisku. Indeksowanie powinno odbywać się w czasie rzeczywistym, a proces ten powinien odbywać się na chronionej stacji, a nie w chmurze. Powiązane ze sobą zdarzenia powinny posiadać unikalny identyfikator, który pomoże zidentyfikować grupę eventów które są ze sobą powiązane. Zapytanie zawierające tego typu identyfikator powinno zwrócić informację o wszystkich zdarzeniach (IP, DNS, PLIKI, REJESTRY, PROCESY, URL itp.) składających się na daną sytuację, niezależnie od tego czy jest ona związana ze złośliwym oprogramowaniem, czy nie. Ponadto dashboard EDR powinien zawierać eksplorator „drzewa procesów" do graficznej wizualizacji i analizy procesów które składały się na dane zdarzenie.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie EDR, które ma możliwość automatycznego i autonomicznego wykonywania wstępnego indeksowania i wstępnego korelowania zdarzeń, w momencie ich wystąpienia w chronionym środowisku. Indeksowanie powinno odbywać się w czasie rzeczywistym. Powiązane ze sobą zdarzenia powinny znajdować się unikalnych incydentach dla danej grupy zdarzeń. Wygenerowane incydenty zawierają incydenty graficzne, Timeline, Detekcje, komputery na których było zdarzenie, pliki wykonywalne oraz procesy składających się na daną sytuację, niezależnie od tego czy jest ona związana ze złośliwym oprogramowaniem, czy nie. Ponadto Detekcje EDR zawierają „drzewa procesów" do graficznej wizualizacji i analizy procesów które składały się na dane zdarzenie.

Odpowiedź: Zamawiający nie zgadza się na zaproponowane rozwiązanie.

Pytanie nr 19

ad. Pkt. 26.

EDR musi być natywnie zintegrowany z komponentem EPP w jednym autonomicznym agencie.
Pytanie:
Czy zamawiający dopuszcza rozwiązanie, które jest zintegrowany z komponentem EPP w jednym autonomicznym agencie, ale działa w postaci usługi systemowej ?

Odpowiedź: Zamawiający dopuszcza zaproponowane rozwiązanie.

Pytanie nr 20

ad. Pkt. 30

Rozwiązanie EPP / EDR musi zapewniać funkcjonalność Full Remote Shell, aby administrator mógł wykonywać polecenia na stacji końcowej, nawet gdy jest ona w stanie izolacji sieciowej. Dodatkowo rozwiązanie musi zapisać transkrypcję zestawionej sesji . Taka transkrypcja musi być chroniona hasłem, a dostęp do powłoki zdalnej powinien wymuszać na Administratorze uwierzytelnianie dwuskładnikowe (2FA) w celu udzielenia dostępu. Funkcjonalność ta powinna być możliwa do włączenia / wyłączenia w polityce bezpieczeństwa rozwiązania.

Pytanie:

Czy zamawiający dopuszcza rozwiązanie, które zapewniać funkcjonalność Full Remote Shell, aby administrator mógł wykonywać polecenia na stacji końcowej, nawet gdy jest ona w stanie izolacji sieciowej. Dodatkowo rozwiązanie musi zapisać transkrypcję zestawionej sesji . Taka transkrypcja jest dostępna tylko z konsoli XDR, do której dostęp jest tylko po podaniu poświadczeń, a dostęp do powłoki zdalnej powinien wymuszać na Administratorze uwierzytelnianie dwuskładnikowe (2FA) w celu udzielenia dostępu.

Odpowiedź: Zamawiający dopuszcza proponowane rozwiązanie, ale wymaga możliwości włączenia / wyłączenia tej funkcjonalności w polityce bezpieczeństwa.

z up. Prezesa Prokuratorii Generalnej RP
Angelika Kraśnicka-Gniewek
Dyrektor Biura Budżetowo-Administracyjnego

Angelika Adriana Kraśnicka-Gniewek

Elektronicznie podpisany przez Angelika Adriana Kraśnicka-Gniewek
Data: 2024.07.16 15:04:28 +02'00'