

Zadanie: Zakup i wdrożenie usługi systemu klasy EDR/XDR

Założenia ogólne

1. Opis zamówienia

- 1.1 Przedmiot zamówienia obejmuje dostarczenie i wdrożenie rozwiązania typu EDR - Endpoint Detection and Response - (zwanego dalej Systemem) wraz z oprogramowaniem, niezbędnymi licencjami oraz świadczenie usługi gwarancji dla wdrażanego systemu.
- 1.2 Zamówienie nie zostało podzielone na części: Zamówienie dotyczy dostawy jednego zintegrowanego systemu wraz z wdrożeniem - jego zakres wymaga, aby wykonywane było ono kompleksowo przez jednego Wykonawcę z uwagi na możliwość wystąpienia niebezpieczeństwa wydłużenia terminu jego realizacji oraz przeciągania się procedur naprawczych w wypadku wystąpienia konieczności usunięcia awarii.

2. Przedmiot zamówienia.

- 2.1 Przedmiotem zamówienia jest Zakup systemu wykrywania oraz reagowania na zagrożenia na stacjach końcowych oraz serwerach.
- 2.2 Realizacja przedmiotu zamówienia polega na dostarczeniu i wdrożeniu rozwiązania typu EDR (Endpoint Detection and Response) (zwanego dalej **Systemem**) wraz z oprogramowaniem, niezbędnymi licencjami oraz świadczeniu usługi gwarancji dla wdrożonego systemu.
- 2.3 W szczególności przedmiot zamówienia obejmuje:
 - a) Dostarczenie najnowszej wersji Systemu.
 - b) Świadczenie usług wsparcia producenta oprogramowania przez okres 14 miesięcy od daty podpisania Protokołu odbioru.
- 2.4 Środowisko Zamawiającego składa się z następujących stacji końcowych:
 - a) Stacji roboczych opartych o system operacyjny z rodziny MS Windows w liczbie do 600 sztuk.
 - b) Serwerów typu Linux i Windows Server w liczbie do 50.
- 2.5 Zamawiający dopuszcza, że w zależności od rodzaju hosta (stacja robocza/serwer) monitorowanie będzie się odbywało za pomocą różnych agentów typu EDR, dedykowanych danej stacji końcowej.

3. Wdrożenie Systemu.

W ramach realizacji Wykonawca dokona wdrożenia Systemu, rozumianego jako:

- 3.1 Instalacja Systemu na czterech serwerach (Windows Server - 2 szt, Linux Centos/Rocky Linux - 1 szt, Linux Debian - 1 szt) oraz dwu stacjach roboczych (Windows 10 – 5 szt, Windows 11 – 5 szt) Szczegóły systemowe zostaną przekazane Wykonawcy po podpisaniu umowy.
- 3.2 Przygotowanie konfiguracji Systemu oraz wdrożenie polityk bezpieczeństwa odzwierciedlających obecnie posiadaną konfigurację i wiedzę o aktualnych zagrożeniach.
- 3.3 Skonfigurowanie logowania zdarzeń na Systemie i umożliwienia zapisywania ich na zewnętrznym serwerze logowania udostępnionym przez Zamawiającego (możliwość zapisywania/eksportu logów w formacie Syslog/CEF/EventLog).
- 3.4 Przeprowadzenie testów funkcjonalnych i bezpieczeństwa zainstalowanego Systemu z udziałem Zamawiającego. Wynikiem testów będzie raport potwierdzający spełnienie zawartych w pkt 5 funkcjonalności Systemu. Raport potwierdzony zostanie przez obie strony.
- 3.5 Za pełne wdrożenie Systemu uznaje się instalację systemu, przeprowadzenie z wynikiem pozytywnym testów akceptacyjnych, funkcjonalnych i bezpieczeństwa, obustronne podpisanie protokołu odbioru

4. Wymagania minimalne dla Systemu EDR:

4.1 Architektura Systemu.

- a) W przypadku dostarczenia Systemu jako maszyny wirtualnej musi być wspierane środowisko Vmware.
- b) Jeżeli System będzie instalowany, jako oprogramowanie na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2012+, Rocky Linux, RHEL.
- c) Jeżeli System będzie dostępny przez interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersji na dzień składania oferty.
- d) Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego (Microsoft Windows 10,

Windows 11, Microsoft Server 2012 i nowszych, macOS oraz Linux (RHEL/Rocky Linux/Debian 9+).

- e) Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania, w tym możliwość wdrożenia rozwiązania przez Zasady Grupy w Windows Server (Group Policy) itp.

4.2 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.

4.3 System 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. System musi wykorzystywać statyczne oraz dynamiczne algorytmy bazujące na sztucznej inteligencji w celu identyfikacji zagrożeń, również tych które nie są wcześniej znane.

4.4 Agent musi być w pełni autonomiczny, co oznacza, że jego działanie i funkcjonalność nie może być zależna od serwera zarządzania, chmury ani ŻADNYCH zasobów zewnętrznych od agenta. Wykrywanie i reagowanie na zaawansowane zagrożenia (0-day, bezplikowe, oparte na pamięci RAM, Exploity 0-Day, ransomware, cryptominers, lateral movement, APT) musi być możliwe w czasie rzeczywistym, nie może zależeć od stanu sieciowego stacji (agent musi realizować te same funkcjonalności w trybie online i offline) oraz nie może wymagać innego rodzaju zewnętrznych zasobów.

4.5 Informacje na temat incydentów bezpieczeństwa muszą być przechowywane co najmniej przez 365 dni.

4.6 Moduły EPP / EDR oferowane przez system muszą automatycznie reagować na pojawiające się zagrożenia, łagodząc zagrożenia w czasie zbliżonym do rzeczywistego, w autonomiczny sposób, z następującymi opcjami odpowiedzi na zagrożenie, definiowane przez politykę bezpieczeństwa:

- a) Ostrzeżenie: taka notyfikacja musi być stała, nawet jeśli polityka nie jest w trybie ochrony.
- b) Zabij proces: Zatrzymuje procesy. Aktywna zawartość w dokumentach, plikach wykonywalnych i procesach podrzędnych jest zatrzymywana. Agent włącza funkcję zabicia procesu dla procesów, które działają wbrew normalnemu zachowaniu stacji końcowej lub nie pasują do działań aplikacji, w której ukrywa się proces.



- c) Kwarantanna: zatrzymuje procesy, szyfruje plik wykonywalny i przenosi go na ograniczoną ścieżkę. Jeśli zagrożenie jest znane, agent automatycznie je unieszkodliwia, zanim będzie można je wykonać.
 - d) Odłącz się od sieci: (kwarantanna sieciowa lub izolacja sieciowa) Agent musi komunikować się tylko z konsolą zarządzającą. Stacja końcowa nie może komunikować się z innymi elementami w sieci. Wszystkie działania na konsoli zarządzania muszą działać niezależnie od stanu izolacji sieci agenta.
 - e) 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.
 - f) Rollback: przywraca stan stacji końcowej do stanu sprzed zmian wprowadzonych 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.
- 4.7 System musi wspierać następujące modele wdrożenia: SaaS (agent-> usługa SaaS w chmurze) lub wdrożenie lokalne (urządzenie wirtualne) lub wdrożenie hybrydowe.
- 4.8 System musi obsługiwać następujące mechanizmy wykrywania złośliwego oprogramowania:
- a) 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 zadań. 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.
 - b) Przed wykonaniem (Pre-Execution): rozwiązanie musi potrafić identyfikować nieznane szkodliwe oprogramowanie oparte na plikach na podstawie analizy statycznej 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.
 - c) 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.

- 4.9 System musi zapewniać silny mechanizm „Anti-Tamper”, czyli mechanizmy ochrony przed manipulacją 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.
- 4.10 Polityka bezpieczeństwa musi zapewniać opcję włączenia lub wyłączenia poszczególnych silników detekcyjnych, lub według typu silnika (silniki przed wykonaniem i uruchomieniem). Opcja ta nie jest wymagana dla silnika reputacji.
- 4.11 System musi zawierać otwarty interfejs API, który umożliwia integracje z innymi rozwiązaniami, monitorowanie środowiska oraz automatyzację niektórych z procesów. Dokumentacja interfejsu API powinna być natywnie dostępna z poziomu konsoli zarządzania.
- 4.12 System musi obsługiwać uwierzytelnianie SSO - SAMLv2.
- 4.13 System musi obsługiwać następujące formaty syslog: CEF, CEF2, RFC-5424, STIX i IOC. System powinno obsługiwać certyfikaty SSL i X.509 do szyfrowania i uwierzytelniania transportu syslog.
- 4.14 System musi zapewniać możliwość wysyłania wiadomości tekstowych do użytkownika stacji końcowej, bezpośrednio z konsoli zarządzania, nawet kiedy agent pracujący na stacji, znajduje się w trybie izolacji sieci / kwarantanny sieciowej.
- 4.15 System 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.
- 4.16 System 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 telemetry, 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.

- 4.17 Polityka ochrony stacji musi umożliwiać odpowiedź na wykryte zagrożenie w oparciu o kwalifikację zdarzenia (zagrożenie [Malicious Threat] czy podejrzané działanie [Suspicious Threat]). Odpowiedź na zagrożenie powinna umożliwiać wybranie opcje alert-only lub opcje aktywnej ochrony w oparciu o klasyfikację zagrożenia. Aktywna odpowiedź na zagrożenie, powinna być wykonywana przez autonomicznego agenta, nawet jeśli chroniona stacja nie jest podłączona do sieci.
- 4.18 System 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.
- 4.19 System 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.
- 4.20 System musi posiadać funkcję informowania o podatnościach aplikacji zainstalowanych na chronionym hoście i dostarczać informacji z CVE związanych z wykrytą podatnością wzbogaconą danymi ze strony MITRE i NVD.
- 4.21 Funkcjonalność przedstawiająca podatności w aplikacjach zainstalowanych na chronionym hoście musi dostarczać informacje o historii danej podatności, to jest, kiedy została wykryta, kiedy została opracowana poprawka, kiedy został przydzielony numer CVE, itp. Dodatkowo funkcja musi przedstawiać indykatory podatności, takie jak np. czy dana podatność jest obecnie używana do wykonywania ataków, czy można ją wykorzystać zdalnie itp.
- 4.22 Przechowywanie danych EDR musi trwać co najmniej 14 dni w modelu opartym na chmurze SaaS i mieć możliwość rozszerzenia do 365 dni.
- 4.23 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 muszą posiadać unikalny identyfikator, który pomoże zidentyfikować grupę zdarzeń, które są ze sobą powiązane. Zapytanie zawierające tego typu identyfikator musi 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 musi

zawierać eksplorator „drzewa procesów” do graficznej wizualizacji i analizy procesów, które składały się na dane zdarzenie.

- 4.24 System musi mieć możliwość szczegółowego definiowania meta danych, które będą zbierane z chronionych hostów (tylko informacje o procesach i zmianach w rejestrze bez kolekcjonowania informacji o operacjach na plikach).
- 4.25 Realizacja modułu EDR musi być zgodna z obowiązującymi dla Zamawiającego przepisami prawa.
- 4.26 EDR musi obsługiwać możliwość tworzenia własnych reguły detekcyjnych. Ta funkcjonalność ma umożliwić analitykowi przekształcenia zapytań (EDR / XDR) w automatyczne reguły detekcyjne, które wyzwalają alerty i automatyczne odpowiedzi, gdy reguły wykryją tego typu zachowanie stacji końcowej.
- 4.27 EDR musi zapewniać przeglądarkę drzewa procesów, w celu uproszczenia i automatyzacji analizy.
- 4.28 System 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.
- 4.29 System musi pozwalać na dodawanie własnych skryptów do centralnego repozytorium wykorzystujących języki Powershell (Windows) i Bash (Linux, Mac).
- 4.30 System musi pozwalać na zdalne uruchomienie skryptów z centralnego repozytorium na wybranych stacjach końcowych. Wynik działania skryptów musi być dostępny lokalnie na stacji końcowej lub w konsoli centralnej.
- 4.31 Konsola centralna musi zapewniać śledzenie stanu działania poszczególnego wywołania skryptu (sukces/porażka/w toku).

5. Instruktaż dla pracowników Zamawiającego

Wykonawca przeprowadzi dla nie więcej niż 6 pracowników Zamawiającego instruktaż, który przygotuje wskazanych pracowników do samodzielnego konfigurowania Systemu, operowania Systemem z poziomu administratora oraz użytkownika oraz wykorzystywania Systemu skonfigurowanego w specyficznej infrastrukturze Zamawiającego, w szczególności do samodzielnej konfiguracji Systemu w celu szybkiego wykrywania działań i zachowań złośliwego oprogramowania oraz badania incydentów bezpieczeństwa za pomocą zdefiniowanych reguł filtrujących / korelacyjnych. Instruktaż będzie trwał minimum 6 godzin zegarowych.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Warunki udziału w postępowaniu

Wykonanie co najmniej dwóch zamówień o wartości minimum 150 000 zł brutto każde w zakresie dostarczenia i wdrożenia rozwiązania typu EDR dla infrastruktury IT klienta przekraczającej 300 stanowisk komputerowych.

Wykonawca spełni warunek jeżeli wykaże w wykazie wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, usług w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, że wykonał należycie co najmniej dwa zamówienia o wartości minimum 150 000 zł brutto każde w zakresie dostarczenia i wdrożenia rozwiązania typu EDR dla infrastruktury IT klienta przekraczającej 300 stanowisk komputerowych.

Kary

Wykonawca za odstąpienie od umowy, niewykonanie lub nienależyte wykonanie zapisów umowy przewiduje zastosowanie kar powszechnie stosowanych dla zamówień tego typu.