Centrum Informatyki Statystycznej

Znak sprawy: CIS-WAZ.271.10.2022
Znak pisma: CIS-WAZ.271.10.2022.1

Warszawa, dnia 22.12.2022 r.

Dotyczy postępowania o zamówienie w trybie przetargu nieograniczonego pt. **Dostawa i wdrożenie systemu EDR (ang. Endpoint Detection and Response) do wykrywania i analizy zaawansowanych zagrożeń CIS-WAZ.271.10.2022**

Centrum Informatyki Statystycznej, na podstawie art. 135 i ust. 1 i 2 ustawy Prawo zamówień publicznych Dz.U. z 2021r poz. 1129 ze zm.), dalej ustawa Pzp, udziela następujących wyjaśnień.

PYTANIE 1.

22. Rozwiązanie musi pozwalać na import pliku STIX w celu wykonania przeszukania bazy danych w poszukiwaniu IoC.

Czy zamawiający zezwala, by w zamian rozwiązanie pozwalało na budowanie podstawowych i zaawansowanych zapytań w celu przeszukiwania zdarzeń, plików, wpisów rejestrze, adresów URL i innych wskaźników IoC w bazie, zgodnie z założonymi parametrami wyszukiwania?

Odpowiedź

Zamawiający podtrzymuje zapis o imporcie plików STIX w celu standaryzacji opisu informacji o zagrożeniach.

PYTANIE 2.

B Metody detekcji

8. System musi być kompatybilny z **otwartym standardem REST API** posiadanego przez Zamawiającego **sandboxa** w celu analizy próbki.

Czy zamawiający zezwala, by w zamian rozwiązanie posiadało możliwość wykorzystania standardu REST API, by móc zintegrować sandbox zamawiającego wraz z systemem klasy EDR?

Odpowiedź

Zamawiający zezwala na rozwiązanie posiadające możliwość wykorzystania standardu REST API do integracji systemu EDR z posiadanym przez Zamawiającego sandboxem w celu analizy próbki.

PYTANIE 3.

C Metody analizy

5. Rozwiązanie musi raportować źródłowe IP, docelowe IP, **C&C**, URL, **klasę złośliwego oprogramowania,** użyte protokoły **i wagę ataku (severity).**

Czy zamawiający zezwala, by w zamian rozwiązanie pozwalało na raportowanie źródłowego i docelowego adresu IP, pliku wykonywalnego , adresów URL, na które odbyło się łączenie, użyte protokoły, nazwę użytkownika, który wywołał zdarzenie, a także proces, który spowodował zdarzenie?

Odpowiedź

Zamawiający zezwala, aby rozwiązanie umożliwiało raportowanie źródłowego i docelowego adresu IP, pliku wykonywalnego, adresów URL, na który odbyło się łączenie, użytego protokołu, nazwy użytkownika oraz procesu, który spowodował zdarzenie.

PYTANIE 4.

7. System musi zastosować właściwe czynności do wywołania aktywności złośliwego oprogramowania. Jako wymaganie minimalne system musi uruchamiać próbkę **wykrywającą wirtualne środowisko w środowisku fizycznym** oraz **oszukiwać próbki, które czekają przez długi czas zanim uruchomią szkodliwe działanie**.

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

Czy zamawiający zezwala, by w zamian rozwiązanie pozwalało na analizę plików w sandbox, który będzie wykrywał różne nietypowe zachowania, w tym minimum wykrywanie środowiska, opóźnienie wykonania, ukrywanie wykonania, listowanie uruchomionych procesów, zamknięcie systemu operacyjnego i inne?

Odpowiedź

Zamawiający w OPZ, w opisie infrastruktury sprzętowo-systemowej podał typ posiadanego sandboxa i traktuje to urządzenie jako integralną część systemu EDR. Jest to fizyczny sandbox Blue Coat Content Analysis System S500-A1.

PYTANIE 5.

D Ochrona urządzenia końcowego

1.System musi umożliwiać użycie blacklisty i whitelisty dla plików definiowanych poprzez wprowadzanie **MD5, SHA256.**

Czy zamawiający zezwala, by w zamian rozwiązanie pozwalało na dodawanie hashy plików do czarnej listy oraz listy wyjątków na podstawie SHA-1?

Odpowiedź

Rozwiązanie musi umożliwiać tworzenie list na podstawie SHA256 i MD5, dodatkowo może wykorzystywać SHA-1.

PYTANIE 6.

12. Musi istnieć możliwość wyboru procesu, dla którego czynności mają zostać pobrane z bufora do konsoli.

Czy zamawiający zezwala, by w zamian rozwiązanie pozwalało na przesyłanie wszystkich zdarzeń z bufora końcówki do serwera zdalnej administracji oraz rozwiązanie pozwoli na filtrowanie ruchu, który ma być niewysyłany z bufora końcówki do serwera

Odpowiedź

Zamawiający podtrzymuje zapisy zawarte w OPZ. System musi mieć możliwość:

- wyboru procesu, dla którego czynności mają zostać pobrane z bufora do konsoli;
- filtracji, które czynności powinny zostać natychmiast wysłane do konsoli zarzadzania, a które powinny zostać przechowywane w buforze urządzenia końcowego.

PYTANIE 7.

17. W przypadku zaoferowania przez Wykonawcę oprogramowania EDR posiadającego wbudowanego klienta ochrony antywirusowej, oprogramowanie to **nie może zakłócać pracy posiadanego przez Zamawiającego oprogramowania AV oraz** systemu operacyjnego a także wypływać na wydajność stacji roboczej.

Czy zamawiający zezwala, by rozwiązanie antywirusowe, obecnie zainstalowane, zostało zmienione na rozwiązanie antywirusowe tego samego producenta, co rozwiązanie EDR. Pozwoli to na lepszą integrację rozwiązań, bez wpływu na wydajność stacji roboczej.

Odpowiedź

Posiadane przez Zamawianego oprogramowanie antywirusowe musi pozostać zainstalowane na urządzeniach końcowych a zainstalowane przez Wykonawcę oprogramowanie EDR nie może zakłócać pracy posiadanego przez Zamawiającego oprogramowania AV oraz systemu.

PYTANIE 8.

Wymagania projektowe

1. W trakcie trwania wdrożenia system ochrony antywirusowej musi działać nieprzerwanie w środowisku Zamawiającego.

Czy zamawiający zezwala, by rozwiązanie antywirusowe zostało zainstalowane natychmiast po ponownym uruchomieniu systemu po deinstalacji poprzedniego rozwiązania antywirusowego.

Taka zmiana oprogramowania antywirusowego nie wpłynie na bezpieczeństwo stacji oraz serwerów.

Odpowiedź

Posiadane przez Zamawianego oprogramowanie antywirusowe musi pozostać zainstalowane na urządzeniach końcowych.

PYTANIE 9.

Szczegółowa specyfikacja prac

12. Dokona integracji z posiadanym przez Zamawiającego sandboxem.

Jakie rozwiązanie posiada zamawiający i na jakim etapie ma odbyć się integracja?

Odpowiedź

Posiadane przez Zamawiającego rozwiązanie typu sandbox zostało opisane w OPZ, w opisie infrastruktury sprzętowo-systemowej. Jest to fizyczny sandbox Blue Coat Content Analysis System S500-A1. Zgodnie z OPZ integracja sandboxa z systemem EDR ma się odbyć na etapie wdrożenia.

PYTANIE 10.

Wymaganie Zamawiającego brzmi: "System musi pracować w środowisku onpremise."
Pytanie:
Czy zamawiający dopuści rozwiązanie on-prem które będzie przechowywać metadane EDR w chmurze publicznej?

Odpowiedź

Zamawiający dopuszcza rozwiązanie, w którym wszystkie komponenty systemu (w tym konsola zarządzająca oraz urządzenia typu appliance jeśli są wymagane) będą zainstalowane on-premise w środowisku obliczeniowym Zamawiającego, natomiast dopuszcza się korzystanie z serwisów reputacyjnych producenta rozwiązania.

PYTANIE 11.

System musi zastosować właściwe czynności do wywołania aktywności złośliwego oprogramowania. Jako wymaganie minimalne system musi uruchamiać próbkę wykrywającą wirtualne środowisko w środowisku fizycznym oraz oszukiwać próbki, które czekają przez długi czas zanim uruchomią szkodliwe działanie.
Pytanie:
Prosimy o doprecyzowanie wymogu. W tym kształcie wskazuje na wymóg sandboxingu próbek.
Czy tak należy to interpretować ?

Odpowiedź

Zamawiający w OPZ, w opisie infrastruktury sprzętowo-systemowej podał typ posiadanego sandboxa i traktuje to urządzenie jako integralną część systemu EDR. Jest to fizyczny sandbox Blue Coat Content Analysis System S500-A1.

PYTANIE 12.

System musi umożliwiać użycie blacklisty i whitelisty dla plików definiowanych poprzez wprowadzanie MD5, SHA256.
Pytanie:
Czy zamawiający dopuszcza możliwość wsparcia tylko dla SHA1 ?

Odpowiedź

Rozwiązanie musi umożliwiać tworzenie list na podstawie SHA256 i MD5, dodatkowo może wykorzystywać SHA-1.

Marcin Piekarek
Dyrektor
Centrum Informatyki Statystycznej

Signed by /
Podpisano przez:

Marcin Piotr Piekarek
Centrum Informatyki
Statystycznej

Date / Data:
2022-12-22 15:32

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl