Centrum Informatyki Statystycznej

Znak: CIS-WAZ.271.1.2024 Warszawa, dnia 21.02.2024 r.

Do zainteresowanych wykonawców

Dotyczy: Postępowania prowadzonego w trybie przetargu nieograniczonego **CIS-WAZ.271.1.2024** na **CIS-WAZ.271.1.2024 na Dostawa i wdrożenie systemu EDR (ang. Endpoint Detection and Response) do wykrywania i analizy zaawansowanych zagrożeń**

Centrum Informatyki Statystycznej działając na podstawie art. 135 ust. 2 ustawy Prawo zamówień publicznych (tj. Dz. U. 2023 poz. 1605 ze zm) dalej „ustawa Pzp", informuje, iż wpłynęły pytania do treści Specyfikacji Warunków Zamówienia (dalej SWZ) i udziela następujących wyjaśnień:

Pytanie 1
Czy zamawiający dopuszcza pełną integrację z systemami SIEM innych producentów przez logowanie danych w równoważnym formacie syslog?

Odpowiedź Zamawiający dopuszcza integrację systemu EDR z rozwiązaniami SIEM przez logowanie danych w równoważnym formacie syslog.

Pytanie 2
Czy zamawiający dopuszcza by rozwiązanie pozwalało na import plików zawierających informację na temat IoC w innym formacie?

Odpowiedź: Zamawiający wymaga możliwości importu w formacie STIX jak również dopuszcza import plików zawierających informację na temat IoC w innym formacie.

Pytanie 3
Czy zamawiający dopuszcza realizację skanowania za pomocą skuteczniejszej i bardziej wydajnej metody opartej na predykcji zamiast skanowania opartego na sygnaturach?

Odpowiedź: Zaoferowane rozwiązanie EDR musi umożliwiać skanowanie sygnaturowe. Zamawiający dopuszcza dodatkowo realizację skanowania za pomocą metod opartych na predykcji.

Pytanie 4
Czy zamawiający dopuszcza użycie bardziej wydajnej techniki pre-execution control zamiast techniki sandboxingu?

Odpowiedź: Zgodnie z wymaganiami w opisie przedmiotu zamówienia (OPZ), zamawiający wymaga zaoferowanie rozwiązania EDR, które musi umożliwiać podłączenie do fizycznego sandboxa on-premise w celu analizy próbki. Zamawiający dopuszcza dodatkowo użycie techniki pre-execution control.

Pytanie 5
Czy zamawiający dopuszcza blokowanie wskazanych aplikacji poprzez poddanie ich kwarantannie?

Odpowiedź: Zamawiający dopuszcza blokowanie wskazanych aplikacji poprzez poddanie ich kwarantannie.

Pytanie 6
Czy zamawiający dopuszcza brak zapory ogniowej w rozwiązaniu EPP+EDR na rzecz integracji z systemową zaporą ogniową urządzenia końcowego?

Odpowiedź: Zamawiający dopuszcza integrację z systemową zaporą ogniową urządzenia końcowego.

Pytanie 7
Czy zamawiający dopuszcza pominięcie tradycyjnego modułu IPS na bazie sygnatur na rzecz bardziej nowoczesnych rozwiązań opartych na regułach MITTRE?

Centrum Informatyki Statystycznej

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

Odpowiedź: Zamawiający podtrzymuje zapis w OPZ (Opis przedmiotu zamówienia) o użyciu modułu IPS na bazie sygnatur.

Pytanie 8
Czy zamawiający dopuszcza by informacje dotycząca integralności nie była przedmiotem osobnego modułu a realizowana jako standardowy proces rozwiązania?

Odpowiedź: Zamawiający dopuszcza by wymagane informacje dotyczące integralności nie były przedmiotem osobnego modułu, mogą być realizowane jako standardowy proces rozwiązania.

Pytanie 9
W związku z ogłoszonym postępowaniem proszę o udzielenie informacji na temat posiadanych oraz wykorzystywanych rozwiązań typu Sandbox. Proszę o wskazanie, czy Zamawiający posiada wdrożone rozwiązanie typu Sandbox, a jeśli tak, to proszę o przedstawienie producenta tego rozwiązania, modelu/typu.

Odpowiedź: Zamawiający w pkt II ppkt 5 „Opis infrastruktury sprzętowo-systemowej…" podał typ posiadanego sandboxa. Jest to fizyczny sandbox Blue Coat Content Analysis System S500-A1.

Pytanie 10
Czy Zamawiający dopuści rozwiązanie Sandbox jako równoważne działające w chmurze?

Odpowiedź: Zamawiający podtrzymuje zapisy w OPZ. System EDR wraz z konsolą zarządzającą musi pracować w środowisku on-premise.

Pytanie 11
Czy Zamawiający dopuści system EDR działający w chmurze i zintegrowany z częścią konsoli ochrony stacji roboczych działającą w trybie on-prem?

Odpowiedź: Zamawiający podtrzymuje zapisy w OPZ. System EDR wraz z konsolą zarządzającą musi pracować w środowisku on-premise.

Pytanie 12
Czy Zamawiający dopuści system równoważny wykorzystujący dedykowany element typu Sandbox bez konieczności integracji po REST API z posiadanym przez Zamawiającego Sandbox'em?

Odpowiedź: Zamawiający podtrzymuje zapisy w OPZ. Zamawiający nie dopuszcza dostarczenia przez wykonawcę dedykowanego elementu typu Sandbox. Zamawiający dopuszcza inne mechanizmy umożliwiające integrację z posiadanym przez zamawiającego urządzeniem Blue Coat Content Analysis System S500-A1.

Pytanie 13
Czy Zamawiający dopuści rozwiązanie, które przeprowadzi analizę behawioralna monitorowanych urządzeń w celu wykrycia i raportowania podejrzanych zachowań wykorzystując moduły korelacji, analizy i interpretacji zdarzeń przez równoważny system chmurowy?

Odpowiedź: Zamawiający nie dopuszcza możliwości wysłania plików do analizy poza infrastrukturę Zamawiającego. Zgodnie z wymaganiami OPZ wszystkie komponenty systemu (w tym konsola zarządzająca, urządzenia typu appliance jeśli są wymagane) będą zainstalowane on-premise w środowisku obliczeniowym Zamawiającego, natomiast dopuszcza się korzystanie z serwisów reputacyjnych producenta rozwiązania.

Pytanie 14
Czy Zamawiający dopuści rozwiązanie równoważne, które umożliwi użycie blacklisty i whitelisty dla plików definiowanych poprzez wprowadzanie MD5, SHA256 przez rozwiązanie chmurowe?

Odpowiedź: Zgodnie z wymaganiami OPZ (Opis przedmiotu zamówienia) zamawiający wymaga aby wszystkie komponenty systemu (w tym konsola zarządzająca, urządzenia typu appliance jeśli są wymagane) będą zainstalowane on-premise w środowisku obliczeniowym Zamawiającego, natomiast dopuszcza się korzystanie z serwisów reputacyjnych producenta rozwiązania, w tym wysyłanie skrótów MD5, SHA256.

Centrum Informatyki Statystycznej

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

Pytanie 15
Czy Zamawiający uważa za równoważne stwierdzenie "poddanie urządzenia końcowego kwarantannie" jako izolację urządzenia końcowego w celu przeprowadzania prac związanych z przeprowadzeniem śledztwa (investigation).

Odpowiedź: TAK, w opinii zamawiającego kwarantanna i izolacja urządzenia są wyrażeniami równoważnymi.

Pytanie 16
Czy Zamawiający pisząc o "module automatycznego wykrywania w sieci nowych, pozbawionych ochrony antywirusowej komputerów i urządzeń sieciowych wysyłający raporty do centralnej konsoli zarządzania" ma na myśli rozwiązania typu NDR bazujcie na kopii ruchu TCP /UDP?

Odpowiedź: Zamawiający nie ma na myśli rozwiązania typu NDR bazującego na kopii ruchu TCP /UDP, chodzi o wykrywanie nowych urządzeń na podstawie rzeczywistego ruchu sieciowego.

Pytanie 17
Dotyczy wymagania "...Projekt techniczny realizacji uzgodnionej koncepcji uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta oprogramowania zawierający:

- model administrowania.

Prosimy o doprecyzowanie wymagania oraz informacje co Zamawiający ma na myśli pisząc o modelu administrowania?

Odpowiedź: Chodzi o wskazanie zaimplementowanych ról administracyjnych RBAC oraz integrację systemu EDR z posiadanymi przez Zamawiającego usługami katalogowymi MS Active Directory.

Pytanie 18
Czy w związku z oferowaniem systemu równoważnego i migracją posiadanego przez Zamawiającego systemu EDR, Wykonawca będzie mógł wnioskować o wydłużenie czasu wdrożenia?

Odpowiedź: Zamawiający podtrzymuje zapisy SWZ.

Marcin Piekarek
Dyrektor
Centrum Informatyki Statystycznej

Signed by / Podpisano przez:
Marcin Piotr Piekarek
Centrum Informatyki Statystycznej
Date / Data:
2024-02-21 15:06

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