Warszawa, 2022-08-11

WPZ.230.2.2022
Identyfikator CeZ: 31472

Do wszystkich Wykonawców

dotyczy: **Zapytania w celu ustalenia szacunkowej wartości zamówienia pn. Zakup systemu służącego do automatyzacji i strukturyzacji procesów w systemach informatycznych Zamawiającego klasy SOAR**, znak sprawy: **WPZ.230.2.2022**, Identyfikator **CeZ:29631**

W związku z faktem, iż do przedmiotowego Zapytania wpłynęły pytania, Zamawiający przytacza treść pytań i udziela odpowiedzi. Jednocześnie Zamawiający dołącza aktualny Załącznik nr 1 do Zapytania – OPZ, w którym zmiany zapisów oznaczone zostały kolorem czerwonym.
Ponadto Zamawiający przesuwa termin na przesłanie odpowiedzi na niniejsze Zapytanie **z dnia 2022-08-12** - **na dzień 2022-08-19 do godz. 16:00.**

Pytanie 1
Dotyczy sekcja I "W ramach zamówienia Wykonawca Wykona" pkt 3 ppkt 3.4 Pojęcie "wybranych podczas dialogu playbook'ów" jest bardzo pojemnie, realnie mamy do czynienia ze scenariuszami od tych bardzo prostych do tych bardzo skomplikowanych i rozbudowanych. W celu przygotowanie rzetelnej wyceny czasochłonności prosimy w miarę możliwości o opisanie planowanych do wykonania scenariuszy wraz oczekiwanymi efektami lub oszacowanie rozkładu 20 planowanych scenariuszy w podziale na krótki, średnio rozbudowany, rozbudowany.

Odpowiedź 1:
Zamawiający przewiduje szacunkowo rozkład 20 planowanych scenariuszy na: 5 (pięć) krótkich scenariuszy, 10 (dziesięć) średnio rozbudowanych scenariuszy i 5 (pięć) rozbudowanych scenariuszy.

Pytanie 2
Dotyczy sekcja I "W ramach zamówienia Wykonawca Wykona" pkt 3 ppkt 3.3 Prosimy o podanie listy integracji z zewnętrznymi źródłami informacji o zagrożeniach i serwisami reputacyjnymi (IOC) z wyszczególnionymi systemami, do których trzeba się podłączyć.

Odpowiedź 2:
Zamawiający wymaga listy zewnętrznych źródeł od Wykonawcy.

Pytanie 3
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 9, czy wystarczającym jest aby rozwiązanie wspierało tylko język python? Elastyczność tego języka pozwala na uruchamianie programów i skryptów napisanych w innych językach, nie tylko wymienionych bezpośrednio w wymaganiu. Wymaganie w obecnym kształcie wskazuje jednoznacznie wskazuje rozwiązanie tylko jednego producenta przez co ogranicza zasadę konkurencyjności.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Odpowiedź 3:
Zamawiający pozostaje przy obecnym zapisie pkt 9. Sekcja III. Wymagania minimalne dla Systemu Załącznik nr 1 do Zapytania – OPZ.

Pytanie 4
Dotyczy sekcja III. Wymagania minimalne dla Systemu pkt 11, Prosimy o dopuszczenie rozwiązania gdzie możliwe jest wykorzystanie dedykowanego i darmowego SDK.

Odpowiedź 4:
Zamawiający dopuszcza możliwość wykorzystania SDK.

Pytanie 5
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 12, Prośba o dopuszczenie systemu, który jest dojrzały i posiada listę instalacji na świecie, bez ograniczenia do konkretnego kraju.

Odpowiedź 5:
Zamawiający pozostaje przy obecnym zapisie pkt 12. Sekcja III. Wymagania minimalne dla Systemu Załącznik nr 1 do Zapytania – OPZ.

Pytanie 6:
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 12.4, Prosimy o dopuszczenie rozwiązania, które obsługuje następujący zestaw produktów z podanej kategorii: CarbonBlack, CrowdStrike Falcon, CylanceProtect, Trend Micro Deep Security, FireEye HX, FortiNet Forti Client EMS, McAfee, Symantec, Vmware Carbon Black, Windows Defender ATP.

Odpowiedź 6:
Zamawiający pozostaje przy obecnym zapisie pkt 12.4. Sekcja III. Wymagania minimalne dla Systemu Załącznik nr 1 do Zapytania – OPZ.

Pytanie 7
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 12.6, Prosimy o dopuszczenie rozwiązania, które obsługuje następujący zestaw produktów z podanej kategorii: VirusTotal, AWS Feed, Cofense, Microsoft Office 365 Feed, Spamhaus, TrendMicro Vision One, STIX, MISP, MITRE ATT&CK, IBM X-Force.

Odpowiedź 7:
Zamawiający dopuszcza następującą listę Repozytoriów Threat Intelligence: VirusTotal, Cofense, Office365, Spamhaus, IBM X-Force, MISP, MITRE ATTACK oraz otwartych formatów: JSON, TXT, CSV.

Pytanie 8:
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 12.7, Prosimy o dopuszczenie rozwiązania, które obsługuje następujący zestaw produktów z podanej kategorii: Cisco, CheckPoint, CrowdStrike, Fortinet, FireEye, TrendMicro, i wiele innych.

Odpowiedź 8:
Zamawiający pozostaje przy obecnym zapisie pkt 12.7. Sekcja III. Wymagania minimalne dla Systemu Załącznik nr 1 do Zapytania – OPZ.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Pytanie 9
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 25, Czy za równoważne rozwiązanie będzie uznany system który pozwala na wersjonowanie scenariuszy oraz uruchamianie ich w trybie debug? Najwygodniejszą metodą pracy z nowymi scenariuszami w celu przetestowania ich poprawności działania jest symulacja działania określonego scenariusza. Proponujemy rozszerzyć wymaganie o możliwość uruchamiania scenariuszy w trybie symulacji.

Odpowiedź 9:
Zamawiający pozostaje przy obecnym zapisie, jednocześnie prosi o doprecyzowanie pytania.

Pytanie 10
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 26, Proponujemy doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy z poziomu GUI oferowanego rozwiązania, bez konieczności każdorazowego odwoływania się do wiersza poleceń co na pewno spowolni pracę operatora oraz obarczy zadanie niepotrzebnym ryzykiem wynikającym z jak najbardziej możliwych błędów składniowych skomplikowanego polecenia.

Odpowiedź 10:
Zamawiający dopuszcza zastosowanie rozwiązania.

Pytanie 11:
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 39, ppkt "wydane komendy i ich rezultaty", Czy poprzez słowo "komenda" zamawiający rozumie operację uruchamianą z CLI lub GUI?

Odpowiedź 11:
Zamawiający poprzez słowo "komenda" rozumie operację uruchamianą z CLI lub GUI.

Pytanie 12:
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 56 wraz podpunktami 1, 2 oraz 3, Prosimy o dopuszczenie rozwiązania, które pozwala na eksport raportów w formacie: pdf oraz json

Odpowiedź 12:
Zamawiający dopuszcza eksport do następujących formatów: PDF, CSV lub JSON.

Pytanie 13:
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 66, Prosimy o dopuszczenie rozwiązania, które posiada możliwość uruchamiania zarówno wbudowanych jak i własnych scenariuszy i automatyzacji w oparciu zarówno o nowe jak i edytowane wskaźniki.

Odpowiedź 13:
Zamawiający dopuszcza rozwiązanie które posiada możliwość uruchamiania zarówno wbudowanych jak i własnych scenariuszy i automatyzacji w oparciu zarówno o nowe jak i edytowane wskaźniki, bez wykorzystania usuniętych wskaźników. Pożądanym przykładem zastosowania jest wywołanie playbook typu threat hunting dla wybranego wskaźnika.

Pytanie 14
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 78, ppkt "komend w ramach danej integracji…", Czy poprzez słowo "komenda" zamawiający rozumie operację uruchamianą z CLI lub GUI?

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Odpowiedź 14:
Zamawiający poprzez słowo "komenda" rozumie operację uruchamianą z CLI lub GUI.

Pytanie 15
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 82, ppkt " sugerowania komend podczas analizy incydentu…", Czy poprzez słowo "komenda" zamawiający rozumie sugestię operacji, którą operator może wykonać?

Odpowiedź 15:
Zamawiający poprzez słowo „komenda" rozumie sugestię operacji, którą operator może wykonać.

Pytanie 16
Dotyczy sekcja III Wymagania minimalne dla Systemu pkt 82, ppkt "podpowiedzi przy tworzeniu scenariuszy (tzw. playbooks)", Wymaganie podpowiedzi przy budowie nowych scenariuszy (tzw playbook'ów) jest w naszej ocenie bardzo trudne do rzetelnej realizacji niezależnie od źródła rekomendacji. Trudno na przykład rekomendować następny krok dla nowo tworzonego scenariusza na podstawie wcześniej skonfigurowanych scenariuszy, poszczególne scenariusze mogą się diametralnie różnić od siebie i każdorazowo wymagają odrębnego projektowania.
W to miejsce proponujemy rozszerzenie wymagania na zastosowanie ML w prezentowaniu podpowiedzi zależnych od wyuczonego modelu dla np: IOC, Kampanie, zadania, assety, incydenty, alarmy, podatności.

Odpowiedź 16:
Zamawiający dopuszcza zastosowanie zaproponowanego rozwiązania w postaci rozszerzenia wymagań na zastosowanie ML w prezentowaniu podpowiedzi zależnych od wyuczonego modelu dla np.: IOC, Kampanie, zadania, assety, incydenty, alarmy, podatności.

Pytanie 17
Czy Centrum e-Zdrowia korzysta z narzędzia ServiceNow?

Odpowiedź 17:
Zamawiający nie korzysta z narzędzia ServiceNow.

Pytanie 18
Ilu użytkowników ma korzystać z systemu SOAR?

Odpowiedź 18:
Zgodnie z zapisami pkt 2. Sekcja I. W ramach zamówienia … Załącznik nr 1 do Zapytania - OPZ.

Pytanie 19
Jakie systemy (liczba, rodzaj) Zamawiającego mają zostać zintegrowane z SOAR w trakcie wdrożenia?

Odpowiedź 19:
Zgodnie z zapisami pkt 12. Sekcja III. Wymagania minimalne dla Systemu Załącznik nr 1 do Zapytania - OPZ.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Pytanie 20
Czy oczekiwane wsparcie dla błędu krytycznego uwzględnia okno 8:00-16:00 Dni Robocze dla przyjmowania zgłoszeń oraz dni robocze dla naprawy?

Odpowiedź 20:
Oczekiwane wsparcie dla błędu krytycznego nie uwzględnia okna między 8:00-16:00 w dni robocze dla przyjmowania zgłoszeń oraz w dni robocze dla naprawy. Zgodnie z pkt 34. Sekcja II. Gwarancja Załącznik nr 1 do Zapytania - OPZ.

Pytanie 21
Jaki poziom integracji jest oczekiwany z systemami IT Ticketing / ITS w tym: OTRS, Jira?

Odpowiedź 21:
Oczekiwany poziom to zakładanie/tworzenie ticketów, zamykanie ticketów.

Pytanie 22
Czy dopuszczacie Państwo rozwiązanie w chmurze (SaaS)? Jakie są Państwa preferencje (rozwiązanie lokalne/w chmurze)?

Odpowiedź 22:
Zamawiający nie dopuszcza rozwiązania w chmurze (SaaS).

2022-08-11
wz. Anny Bułhak
(-) Sabina Ryszka

(data, podpis kierownika WPZ)

Sporządziła: Iwona Balcerzak

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706