Załącznik nr 1 do Zapytania

Identyfikator CeZ:29631

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: **Zakup systemu służącego do automatyzacji i strukturyzacji procesów w systemach informatycznych Zamawiającego klasy SOAR.**

Realizacja przedmiotu zamówienia polega na dostarczeniu i wdrożeniu rozwiązania typu SOAR (Security Orchestration, Automation And Response) zwanego dalej „Systemem" wraz z Oprogramowaniem, niezbędnymi licencjami oraz świadczeniu usługi gwarancji dla wdrożonego Systemu.

Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 30 Dni Roboczych, liczonym od dnia zawarcia Umowy.

I. W ramach zamówienia Wykonawca:

1. Przygotuje Projekt Techniczny w terminie 5 Dni Roboczych od daty podpisania Umowy, zawierający w szczególności:
   1.1. harmonogram realizacji Przedmiotu Umowy,
   1.2. szczegółowy opis architektury Systemu,
   1.3. opis funkcjonalny Systemu,
   1.4. opis sposobu instalacji i konfiguracji Systemu w lokalizacji Zamawiającego.
2. Dostarczy najnowszą wersję Systemu oraz licencje Oprogramowania wraz z licencją dostępową dla minimum dwóch użytkowników oraz zapewnieni świadczenie usług gwarancyjnych producenta przez okres nie krótszy niż 12 miesięcy i nie dłuższy niż 36 miesięcy od daty podpisania Protokołu odbioru.
3. Skonfiguruje i zainstaluje Oprogramowanie dostarczone w ramach Systemu, w tym dokona:
   3.1. instalacji dostarczonego Oprogramowania,
   3.2. konfiguracji Oprogramowania w infrastrukturze Zamawiającego,
   3.3. konfiguracji, dostarczonych przez Zamawiającego, integracji z zewnętrznymi źródłami informacji o zagrożeniach i serwisami reputacyjnymi (IOC),
   3.4. konfiguracji 20 wybranych podczas dialogu playbook'ów (procesów automatyzacji).
4. Przeprowadzi testy poprawności działania zainstalowanego i skonfigurowanego Systemu.
5. Stworzy dokumentację powykonawczą.
6. Przeprowadzi instruktaż stanowiskowy z obsługi oraz administracji Systemu dla maximum 12 administratorów (minimum 3 Dni Robocze, łącznie minimum 24 godziny zegarowe). Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu. Instruktaż będzie realizowany w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu. Lista osób oraz termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą drogą mailową po podpisaniu Umowy.
7. Za pełne wdrożenie Systemu uznaje się instalację Systemu, przeprowadzenie z wynikiem pozytywnym testów, o których mowa w pkt 4, integrację z systemami Zamawiającego, dostarczenie kompletu dokumentacji, przeprowadzenie Instruktażu opisanego w pkt 6, obustronne podpisanie Protokołu odbioru.

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

II. Gwarancja

Zapisy ogólne

1. Wykonawca udziela Zamawiającemu Gwarancji na:
   1.1. Wdrożony System.
   1.2. Oprogramowanie.
2. Wykonawca oświadcza, że Oprogramowanie przez niego dostarczone objęte jest gwarancją producenta.
3. Wykonawca udziela gwarancji na elementy wymienione w pkt I. ppkt 2, która obowiązuje przez okres nie krótszy niż 12 miesięcy i nie dłuższy niż 36 miesięcy od daty podpisania Protokołu odbioru, wskazanego w Umowie.
4. Wykonawca zobowiązany jest w okresie realizacji Umowy do usuwania Błędów elementów wymienionych w pkt I. ppkt 2 na zasadach opisanych w niniejszym załączniku.
5. Zakres świadczeń w ramach Gwarancji obejmuje:
   5.1. usuwanie Błędów elementów wymienionych w pkt I. ppkt 2 zgodnie z Czasami Reakcji, Czasami Naprawy, Czas Propozycji Rozwiązania i dla poszczególnych kategorii Błędów,
   5.2. dostarczanie nowych wersji Oprogramowania,
   5.3. aktualizację Dokumentacji w przypadku wprowadzania zmian w Systemie lub Oprogramowaniu w wyniku naprawy Błędu, w terminie 5 Dni Roboczych od dnia naprawy.
6. Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych z wykorzystaniem Systemu.
7. W ramach świadczenia przez Wykonawcę usług w ramach Gwarancji, Wykonawca zobowiązany jest do umożliwienia osobom wskazanym przez Zamawiającego obserwacji prac Wykonawcy.
8. W przypadku wykrycia przez Zamawiającego Błędu, Zamawiający dokona kwalifikacji zgłoszenia (Błąd Krytyczny/Błąd Zwykły) według własnego uznania na podstawie zdefiniowanych kryteriów. Zgłoszenie zawierać będzie posiadane przez Zamawiającego informacje na temat nieprawidłowego działania Systemu istotne w ocenie Zamawiającego dla zdiagnozowania i usunięcia nieprawidłowości w działaniu Systemu.
9. Formalne potwierdzenie Zgłoszenia stanowi przesłanie przez Zamawiającego do Wykonawcy informacji o wystąpieniu Błędu i opisie jego symptomów.
10. Wykonawca zobowiązuje się rejestrować zgłaszane Błędy wykorzystując rozwiązania umożliwiające raportowanie Zgłoszeń - w tym Czas Reakcji, Czas Propozycji Rozwiązania oraz Czas Naprawy.
11. Wykonawca będzie przyjmował Zgłoszenia przez cały czas, tj. w systemie 8:00-16:00 Dni Robocze.
12. Wykonawca będzie przyjmował Zgłoszenia przekazywane w jeden z następujących sposobów:
    12.1. za pomocą aplikacji serwisowej (interfejsu serwisowego),
    12.2. przez przesłanie Zgłoszenia pocztą elektroniczną na adres: ……@.....
13. W razie otrzymania przez Wykonawcę Zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Błędu z innego źródła niż Zgłoszenie, Wykonawca zobowiązany będzie do podjęcia działań zmierzających do usunięcia Błędu.
14. Jeżeli Zamawiający nie wie o istnieniu Błędu, Wykonawca poinformuje w ciągu 24 godzin, Zamawiającego o jego wystąpieniu.

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

15. Jeżeli Wada została wykryta przez Wykonawcę, Wykonawca nada jej odpowiednią wstępną kategorię (Błąd Krytyczny / Błąd Zwykły). W ciągu 2 godzin od powiadomienia przez Wykonawcę Zamawiający ma prawo zmienić kategorię Błędu.
16. Ostatecznie o klasyfikacji kategorii Błędu (Błąd Krytyczny / Błąd Zwykły) decyduje Zamawiający.
17. Wykonawca zobowiązany jest do potwierdzenia przyjęcia Zgłoszenia odpowiednim wpisem we własnej aplikacji serwisowej (dotyczy to również Zgłoszeń składanych pocztą elektroniczną) oraz o nadaniu indywidualnego identyfikatora zgłoszenia. Chwila potwierdzenia przyjęcia Zgłoszenia nie ma wpływu na Czas Reakcji, Czas Propozycji Rozwiązania, Czas Naprawy. Wykonawca jest zobowiązany do udostępnienia Zamawiającemu własnej aplikacji serwisowej w zakresie przeglądania Zgłoszeń związanych z realizacją Umowy.
18. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Systemu, którego dotyczy Zgłoszenie nie jest spowodowane Błędem, za który odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest:
    18.1. wskazać przyczynę nieprawidłowego działania poprzez wskazanie elementu, który ją powoduje,
    18.2. udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji o Systemie lub Oprogramowaniu potrzebnych do przywrócenia pełnej funkcjonalności.
19. Po przeprowadzeniu Naprawy, Wykonawca zgłosi ją do odbioru poprzez przekazanie informacji :
    19.1. za pomocą aplikacji serwisowej (interfejsu serwisowego),
    19.2. przez przesłanie pocztą elektroniczną na adres: ……@.....
20. Po weryfikacji dokonania Naprawy, przedstawiciel Zamawiającego niezwłocznie potwierdzi w systemie lub drogą elektroniczną skuteczność lub nieskuteczność Naprawy. Data i godzina rejestracji w systemie lub wysłania maila przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi Naprawy.
21. W przypadku stwierdzenia dokonania skutecznej Naprawy Wykonawca zamyka Zgłoszenie i potwierdza jego wykonanie poprzez „zamknięcie” zgłoszenia w aplikacji serwisowej.
22. Naprawa, co do której Wykonawca poinformował o jej wykonaniu, a która została odrzucona przez przedstawiciela Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Błąd nadal występuje, trwa do czasu jej skutecznego wykonania.
23. Wykonawca zobowiązany jest do prowadzenia ewidencji otwartych i zamkniętych Zgłoszeń, obejmującej w szczególności opis stanu realizacji danej Naprawy. Powyższe dane dostępne są cały czas dla Zamawiającego za pośrednictwem aplikacji serwisowej.
24. Wraz z dokonaniem Naprawy Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu odpowiednie Dokumenty, o ile zachodzi taka potrzeba.
25. Jeżeli Wykonawca nie dokona Naprawy Błędu w określonym terminie to Zamawiający może według swojego uznania:
    25.1. zawiadamiając uprzednio Wykonawcę usunąć Błąd we własnym zakresie lub powierzyć jej usunięcie innym podmiotom trzecim na ryzyko i koszt Wykonawcy, co nie spowoduje utraty przysługujących Zamawiającemu uprawnień z tytułu Gwarancji – przy czym koszty poniesione przez Zamawiającego przy usunięciu Błędu mogą być potrącone z wynagrodzenia

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

przysługującego Wykonawcy lub z zabezpieczenia należytego wykonania przedmiotu Umowy, na co Wykonawca wyraża zgodę lub

25.2. obciążyć Wykonawcę karą umowną.

26. Jeżeli w trakcie realizacji zobowiązań z tytułu Gwarancji dojdzie do wprowadzenia zmian w Dokumentach, wówczas do przejścia autorskich praw majątkowych do zmienionych Dokumentów stosuje się odpowiednio postanowienia Umowy, w zakresie Dokumentów będących wynikiem zmian. W zakresie Oprogramowania lub jego dokumentacji, ich producent z chwilą wykonania zobowiązań z tytułu gwarancji udziela licencji na zasadach określonych w Umowie.
27. W uzasadnionych przypadkach Strony mogą podjąć decyzję o wydłużeniu Czasu Naprawy.
28. Warunki Gwarancji dla Oprogramowania.
29. Gwarancją objęta jest całość dostarczonego Oprogramowania.
30. Wykonawca zapewni elektroniczny dostęp do informacji na temat dostarczonego Oprogramowania oraz biuletynów technicznych, poprawek, aktualizacji, nowych wersji Oprogramowania.
31. W przypadku Oprogramowania:
    31.1. Wykonawca zapewnia Zamawiającemu dostarczanie aktualizacji, nowych wersji oraz zmian Oprogramowania/opracowanych przez producentów w okresie gwarancji. Wykonawca zapewnia, że dostarczane aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim na zasadach określonych w niniejszym załączniku oraz Umowie.
    31.2. aktualizację Oprogramowania, w szczególności dostarczania i instalacji nowych wersji Oprogramowania systemowego i Oprogramowania, dostarczania i instalacji wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych.
    31.3. Informuje o najlepszych praktykach i zasadach postępowania.
32. Poziomy SLA dla Oprogramowania/Systemu

Kategoria Błędu (priorytety)	**Czas Reakcji** (od momentu zgłoszenia)	**Czas Propozycji Rozwiązania** (od momentu potwierdzenia)	**Czas Naprawy** (od momentu zgłoszenia)
Błąd Zwykły	1 Dzień Roboczy	1 Dzień Roboczy	3 Dni Robocze
Błąd Krytyczny	2 godziny	12 godzin	24 godziny

33. Zgłoszenie o zwykłym priorytecie (Błąd Zwykły) - w zakresie błędów związanych z Oprogramowaniem/Systemem z czasem reakcji maksymalnie 1 Dzień Roboczy od chwili zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 1 Dni Roboczy od dnia potwierdzenia zwrotnego przyjęcia zgłoszenia (przez Dni Robocze rozumie się dni od poniedziałku do piątku w godzinach 8:00-16:00, z wyjątkiem dni ustawowo wolnych od pracy i dni wolnych od pracy u Zamawiającego). Rozwiązanie problemu o priorytecie zwykłym przez Wykonawcę nastąpi w terminie nie przekraczającym 3 Dni Robocze od zgłoszenia Błędu Zwykłego.

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

34. Zgłoszenie o krytycznym priorytecie (Błąd Krytyczny) - obejmujące pomoc przy wykryciu na serwerach produkcyjnych błędów krytycznych, konfiguracji Oprogramowania z czasem reakcji maksymalnie 2 godziny od chwili zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 12 godzin od momentu potwierdzenia zwrotnego przyjęcia zgłoszenia. Rozwiązanie problemu o priorytecie krytycznym przez Wykonawcę nastąpi w terminie nie przekraczającym 24 godziny od momentu zgłoszenia Błędu Krytycznego.
35. W ramach Gwarancji w okresie nie krótszym niż 12 miesięcy i nie dłuższym niż 36 miesięcy od daty odbioru wdrożenia Systemu, Wykonawca wykona dodatkowe automatyzacje (playbook'ów). Nie mniej niż 12 i nie więcej niż 36 automatyzacji (playbook'ów) z założeniem maksymalnie jedna automatyzacja (playbook'i) na miesiąc.
36. W ramach Gwarancji od Wykonawcy wymagane jest:
    36.1. aktualizacja Systemu,
    36.2. dostęp do nowych wersji Systemu oraz poprawek,
    36.3. dostęp do nowych sygnatur bezpieczeństwa,
    36.4. wsparcie w rozwiązywaniu problemów z dostarczonym oprogramowaniem,
    36.5. dostęp do bazy wiedzy producenta.
37. Okresowe przeglądy Systemu. W ramach realizacji Gwarancji, Wykonawca będzie świadczył okresowe przeglądy Systemu, nie rzadziej niż 3 miesiące, polegające na:
    37.1. przeglądzie poprawek dla eksploatowanych środowisk wykorzystujących System,
    37.2. ocenie konieczności zastosowania poprawek rekomendowanych przez producenta oprogramowania w eksploatowanych środowiskach oraz ich wdrożenie,
    37.3. doradztwie architektonicznym w zakresie zgodności sposobu wykorzystywania oprogramowania z najlepszymi praktykami rekomendowanymi przez dostawcę oraz zgodności z warunkami Umowy,
    37.4. informowaniu Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu,
    37.5. doradztwie technicznym, przekazywaniu na bieżąco informacji o nowych funkcjonalnościach możliwych do zaimplementowania w oprogramowaniu,
    37.6. założeniu zgłoszenia w serwisie pomocy technicznej producenta, w przypadku wad i błędów oprogramowania, przekazanie zgłoszenia serwisowego do producenta oprogramowania oraz prowadzenie zgłoszenia w imieniu Zamawiającego,
    37.7. wsparciu w konfiguracji i optymalizacji Systemu.

III. Wymagania minimalne dla Systemu:

Oferowany System musi:

1. Być systemem klasy SOAR (Security Orchestration, Automation and Response) wspierającym zespół analityków bezpieczeństwa SOC w efektywnym zarządzaniu procesem obsługi incydentów poprzez integrację różnych wykorzystywanych produktów i narzędzi automatyzując przepływ informacji między nimi celem przyspieszenia odpowiedzi na zagrożenie.
2. Pochodzić od jednego producenta, być jednym, w pełni zintegrowanym systemem klasy SOAR, pokrywającym funkcjonalności:
    2.1. Security Orchestration and Automation (SOA),
    2.2. Security Incident Response Platform (SIR),

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

2.3. Threat Intelligence Platform (TIP),
zgodnie z definicją firmy Gartner.

3. Umożliwiać przypisanie obsługi incydentu do użytkownika lub zespołu analityków bazując na zdefiniowanych rolach w systemie oraz określić termin rozwiązania problemu (tzw. metrykę SLA).
4. Umożliwiać dwustronną komunikację z użytkownikami systemu (np. w celu zebrania dodatkowych informacji od osób związanych z incydentem) oraz operatorami systemu SOAR, na przykład poprzez zastosowanie interaktywnych formularzy.
5. Zapewniać zestaw co najmniej 100 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.
6. Pozwalać na odbieranie danych z zewnętrznych systemów klasy ITS (https://en.wikipedia.org/wiki/Issue_tracking_system) i wykorzystywać je zarówno do tworzenia nowych incydentów jak również wzbogacania dodatkowymi danymi tych już istniejących.
7. Automatyzować proces analizy otrzymanych danych, realizować funkcje informacyjne, jak również podejmować funkcje naprawcze (np. automatyczna analiza pliku w chmurze sandbox wybranego producenta, wysłanie wiadomości e-mail do użytkownika zainfekowanej stacji końcowej, aby nie otwierał załącznika i blokada na urządzeniu sieciowym dostępu do wskazanych usług dla wybranego użytkownika).
8. Posiadać wbudowaną bibliotekę minimum 20 typów incydentów, a także powinno dostarczać specjalizowane typy incydentów związane z integrowanymi systemami, pozwalając jednocześnie na ich edycję lub kopiowanie celem stworzenia własnej karty incydentu. Dopuszczalne jest rozwiązanie, które ma poniżej 20 gotowych typów incydentów, ale które na etapie wdrożenia może utworzyć dowolną ilość typów incydentów bez konieczności prowadzenia żadnych prac developerskich, o ile nie przełoży się to negatywnie na termin realizacji Przedmiotu Umowy.
9. Pozwalać na wykorzystanie języków skryptowych (co najmniej Python, Javascript, Powershell) w celach automatyzacji zadań.
10. Umożliwić wykorzystanie w skryptach własnych bibliotek zewnętrznych oraz programów (np. poprzez umożliwienie uruchomienia skryptów we własnym kontenerze, zawierającym pożądane oprogramowanie).
11. Zapewnić integrację (np. przy pomocy wtyczek) z popularnymi programami klasy IDE (ang. Integrated DeveLopment Environment) np. PyCharm, w celu ułatwienia edycji skryptów. Integracja może zostać zrealizowana na etapie wdrożenia.
12. Być dojrzały w rozumieniu ilości już potwierdzonych wdrożeń na polskim rynku oraz zapewniać gotową integrację wiodących produktów i usług z zakresu bezpieczeństwa IT, w tym:
    12.1. Microsoft Active Directory,
    12.2. narzędzi komunikacyjnych np. serwerów pocztowych, Slack, GSuite itp.,
    12.3. systemów klasy SIEM i analizy logów w tym: IBM QRadar, McAfee, RSA Netwitness, Splunk itp.,
    12.4. systemów ochrony stacji końcowych klasy EPP (https://www.gartner.com/it-glossary/endpoint-protection-platform-epp/) uwzględniających funkcje blokowania, jak również analizy i odpowiedzi w tym: Fidelis EDR, FireEye HX, McAfee, RSA Netwitness EndPoint, Symantec, TrendMicro Deep Security,
    12.5. systemów bezpieczeństwa sieciowego typu firewall, NGFW, IPS/IDS,
    12.6. repozytoriów Threat Intelligence w tym: VirusTotal, Cofense, Azure/Office365 feeds, Spamhaus, ProofPoint, MISP, MITRE ATTACK, IBM X-Force oraz otwartych formatów: JSON, TXT, CSV,

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

12.7. narzędzi typu forensics i systemów sand-box w tym: Fortinet, FireEye, Palo Alto Networks Wildfire, Volatility, itp.,
12.8. zewnętrznych baz danych w tym: PostgreSQL, MySQL, MangoDB, Microsoft SQL, Elastic,
12.9. systemów IT Ticketing / ITS w tym: OTRS , Jira itp.,
12.10. skanerów podatności w tym: Qualys, Nessus.

13. Zapewniać możliwość wglądu w kod integracji oraz jego klonowanie pod kątem wprowadzania modyfikacji lub napisania własnej wersji integracji (tzw. wsparcie modelu BYOI - Bring Your Own Integration).
14. Zapewniać co najmniej 100 prekonfigurowanych, gotowych scenariuszy użycia (ang. playbooks) pozwalających na ich natychmiastowe wykorzystanie do automatycznej obsługi incydentu bezpieczeństwa.
15. Pozwalać na kopiowanie oraz edycję już istniejących scenariuszy jak również dodawanie nowych.
16. Pozwalać na edycję i dodawanie nowych scenariuszy obsługi incydentu (tzw. playbook) za pomocą graficznego interfejsu użytkownika bez konieczności wykorzystania języków skryptowych lub znajomości języków programowania.
17. Pozwalać na tworzenie scenariuszy zagnieżdżonych, tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane na zasadzie pod-scenariuszy. Edycja/zmiana pod-scenariusza wpływa automatycznie na wszystkie scenariusze, które go wykorzystują, co ułatwia administrację.
18. Pozwalać na tworzenie scenariuszy zawierających:
    - zadania ręczne,
    - zadania zautomatyzowane,
    - zadania warunkowe automatyczne,
    - zadania warunkowe ręczne,
    - akwizycję danych przy użyciu formularzy,
    - filtry danych,
    - pod-scenariusze.
19. Pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy.
20. Pozwalać na automatyczne dokumentowanie uruchomionych scenariuszy wraz z wynikami jego działania.
21. Umożliwiać wizualizacje przebiegu wykonania scenariusza (wizualizacje rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.).
22. Pozwalać na sterowanie wykonaniem scenariusza przez operatora (zadania warunkowe ręczne) zarówno przy użyciu graficznego interfejsu użytkownika, jak i drogą korespondencyjną (m.in. z poziomu wiadomości email oraz wiadomości w komunikatorze takim jak np. Microsoft Teams, itp.).
23. Pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów.
24. Pozwalać na ponowne uruchomienie scenariusza na konkretnym incydencie, jeżeli zajdzie taka potrzeba.
25. Pozwalać na zatrzymanie scenariusza w trakcie jego wykonania, zmianę rezultatu wybranych operacji warunkowych w scenariuszu, dodanie dodatkowych zadań oraz ponowienie / modyfikację wybranych zadań bez konieczności ponownego uruchomienia całej procedury obsługi scenariusza.
26. Pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń).

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

27. Pozwalać na proste monitorowanie stanu wykonania scenariuszy powiązanych z incydentami. Ponadto, w przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza, osoby odpowiedzialne za incydent powinny zostać natychmiast o tym poinformowane.
28. Pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.
29. Pozwalać na przekazywanie parametrów pomiędzy zadaniami pojedynczego scenariusza.
30. Pozwalać na odczytywanie wyników działania pod-scenariuszy i wykorzystaniu ich w kolejnych zadaniach uruchomionego scenariusza.
31. Pozwalać na sprawdzenie historycznych danych na temat uruchomionych scenariuszy/zadań.
32. Pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i wedle harmonogramu.
33. Pozwalać na przydzielenie konkretnego zdarzenia do konkretnego członka zespołu SOC zarówno ręcznie jak i automatycznie, na podstawie różnych kryteriów, m. in.: aktualne obciążenie operatora, dostępność operatora według zdefiniowanego czasu pracy, inteligentne sugestie oparte o uczenie maszynowe, dostępność operatora w oparciu o to czy jest zalogowany do interfejsu systemu SOAR, itp.
34. Pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.
35. Pozwalać na tworzenie własnych:
    - typów incydentów,
    - pól/etykiet incydentów,
    - typów wskaźników (ang. indicator),
    - pól/etykiet wskaźników (ang. indicator),
    - raportów,
    - dashboardów.
36. Pozwalać na automatyczne generowanie karty incydentu zgodnej z wzorem dokumentu, dostarczonym przez zamawiającego.
37. Pozwalać na automatyczne wypełnianie pól incydentu bazując na typie incydentu lub jego atrybutach.
38. Pozwalać na delegowanie zadań innym członkom zespołu SOC w ramach oceny danego incydentu.
39. Pozwalać na dokumentowanie następujących informacji:
    - zmiany wykonane dla konkretnego incydentu,
    - członkowie zespołu zajmujący się incydentem,
    - wydane komendy i ich rezultaty,
    - wykonane zadania scenariuszy i ich rezultaty.
40. Pozwalać na zapisywanie historycznych incydentów wraz z pełną informacją na temat podjętych akcji obsługi/rozwiązania w celu szkolenia/transferu wiedzy pomiędzy członkami zespołu SOC (Na historię incydentu składają się wyniki działania automatycznych i ręcznych zadań określonych w playbooku, komentarze analityków pracujących nad incydentem, wyniki komend wykonywanych przez analityków w czasie obsługi incydentu z użyciem linii poleceń (CLI), indykatory zagrożenia IOC (IP, URL, domeny, itd.) wyciągane automatycznie i wskazywane ręcznie w czasie obsługi incydentu, elementy analizy oznaczone przez analityków jako dowód w sprawie (np. zrzuty ekranu z widokiem podejrzanych stron web), pliki dodawane do historii obsługi incydentu przez analityków, itp.).
41. Musi istnieć możliwość zbiorczego importu i eksportu wskaźników IOC bezpośrednio z GUI.
42. Pozwalać na przechowywanie wskaźników (ang. indicator) w centralnym miejscu i przedstawienia ich korelacji pomiędzy incydentami. Korelacja powinna być obustronna, tzn. jakie wskaźniki posiada wybrany incydent lub z jakimi incydentami powiązany jest wybrany wskaźnik.

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

43. Pozwalać na import wskaźników kompromitacji z serwerów TAXII 1.x, 2.0, 2.1 oraz ich eksport w formatach STIX i CSV.
44. Pozwalać na tworzenie wielu instancji integracji tego samego typu do rozwiązań firm trzecich (przykładowo dwie integracje z serwerami IMAP lub zaczytujące dane threat intel z dwóch źródeł w formacie JSON).
45. Pozwalać na zdefiniowanie reguł wstępnego przetwarzania (pre-process rules) lub analogicznego mechanizmu, pozwalającego na deduplikację, zamknięcie lub odrzucenie nowo zgłoszonych incydentów, przed rozpoczęciem procedury ich obsługi (m.in. celem odciążania systemu w przypadku wystąpienia bardzo dużej liczby redundantnych incydentów).
46. Pozwalać na rozszerzenie możliwości systemu w zakresie tworzenia i edycji scenariuszy poprzez dodanie własnych skryptów realizujących niestandardową logikę operacji warunkowych, filtracji danych, modyfikacji danych, a także skryptów realizujących niestandardową prezentację danych w dashboardach, zadania wykonywane po zakończeniu obsługi incydentu itp.
47. Producent Systemu musi dostarczać własną bazę CTI (Cyber Threat Intelligence). Integracja z CTI musi umożliwiać pobieranie przez System informacji o aktualnych danych związanych z zagrożeniami występujących w cyberprzestrzeni (listy reputacyjne adresów IP, adresów DNS, skróty (sumy kontrolne) złośliwego oprogramowania oraz złośliwych plików, itp.).
48. System musi posiadać możliwość definiowania w sposób ustrukturyzowany danych o Incydencie w postaci artefaktów. Co najmniej muszą być wspierane domyślnie następujące rodzaje:
    - pliki,
    - skróty danych w postaci SHA1, SHA256, MD5,
    - adresy IP,
    - adresy URL,
    - nazwy DNS,
    - Hostname,
    - Port,
    - Rejestr,
    - Użytkownik,
    - Proces,
    - adres email.
49. System musi posiadać zestaw przygotowanych raportów takich jak:
    - Raport na temat incydentów: dzienny, 7- i 30-dniowy,
    - Raport na temat średniego czasu rozwiązania incydentu,
    - Raport podsumowania zmiany SOC,
    - Raport otwartych i opóźnionych incydentów.
50. Pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację pożądanych danych (np. wykres kołowy, słupkowy, liniowy, tabela itp.).
51. Pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego języka zapytań) oraz podobieństwa do innych incydentów (related incidents).
52. Pozwalać na wizualizację zależności pomiędzy podobnymi incydentami na poziomie wystąpień identycznych indykatorów.
53. Pozwalać na oznaczenie najważniejszych informacji o incydencie, celem wyróżnienia ich w raporcie oraz w interfejsie graficznym.

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

54. System musi umożliwiać analitykowi analizę graficzną powiązań pomiędzy incydentami i IOC. Graficzna korelacja musi być dostępna dla różnych typów rekordów np. assety, podatności, alarmy, incydenty.
55. Pozwalać na tworzenie własnych raportów oraz kart incydentów poprzez uzupełnienie dostarczonego przez klienta wzorca dokumentu np. w formacie .docx.
56. Pozwalać na eksport raportów w formacie:
    56.1. PDF,
    56.2. DOC,
    56.3. CSV.
57. Pozwalać na tworzenie własnych dashbordów zawierających informacje o:
    - kondycji SOC i powiązanych ryzyku biznesowym (MTTR/MTTD),
    - produktywności członków zespołu SOC,
    - ilości i statusu incydentów (właściciel, typ, czas rozwiązania, itp.),
    - kondycji systemu SOAR (np. wykorzystaniu pamięci, CPU itp.).
58. Pozwalać na uwierzytelnianie dwuskładnikowe.
59. Pozwalać na audyt aktywności członków zespołu SOC.
60. Mieć możliwość działania jako platforma SOAR dla wielu instytucji/klientów z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant).
61. Mieć możliwość: kooperacji między systemem zarządzającym (master) a systemem klienta (tenant) z wyizolowanymi możliwościami wykonania, tworzenia scenariuszy na systemie zarządzającym dla wielu systemów klienckich, wspólnych analiz incydentów w celu zredukowania średniego czasu do rozwiązania - MTTR (mean time to resolve).
62. Mieć możliwość selektywnego dystrybuowania treści do systemów klienckich (takich jak scenariusze, integracje, raporty).
63. Mieć możliwość współdzielenia wskaźników (ang. indicators) między systemami klienckimi.
64. Posiadać repozytorium wskaźników (ang. indicators), które kolekcjonuje i koreluje wskaźniki w ramach wszystkich incydentów, alertów i feedów dostarczanych do rozwiązania.
65. Posiadać możliwość wykonywania scenariuszy na podstawie zestawu wskaźników (ang. indicators) określonych przez użytkownika.
66. Posiadać możliwość uruchamiania zarówno wbudowanych jak i własnych scenariuszy i automatyzacji w oparciu o nowe/edytowane/usunięte wskaźniki. Pożądanym przykładem zastosowania jest wywołanie playbook typu threat hunting dla wybranego wskaźnika.
67. Być w stanie obsługiwać formaty strukturalne, takie jak JSON, CSV, STIX 1.X i STIX 2.X itp. W ramach integracji ze źródłami wskaźników (ang. indicators). Może także obsługiwać formaty niestrukturalne, takie jak poczta e-mail, wiadomości, kanały RSS i inne.
68. Wspierać minimum następujące typy wskaźników (ang. indicators):
    - adres email,
    - konto użytkownika,
    - wyniki CVE,
    - domena,
    - FQDN,
    - nazwy hosta,
    - IP (v4 oraz v6),
    - klucz i ścieżka rejestru,
    - URL,

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

- CIDR.

69. Umożliwiać własną definicję wskaźników, jego pól oraz skryptów reputacyjnych.
70. Realizować de-duplikację wskaźników.
71. Zapewniać użytkownikom możliwość automatycznej weryfikacji wskaźników (tzw. enrichment), wykonując odpowiedni scenariusz lub uruchamiając sprawdzanie na podstawie typu wskaźnika (ang. indicator).
72. Umożliwiać wdrożenie zarówno lokalnie (tzw. on-premise server) na fizycznej platformie serwerowej, jak również w wirtualnej infrastrukturze (w prywatnym DC) wspierać co najmniej środowiska producentów VMware lub udostępnianej z chmury publicznej w modelu SaaS.
73. Wspierać instalację w trybie pracy standardowym, jak i multi-tenant.
74. Zapewniać możliwość tworzenia automatycznych, okresowych kopii zapasowych.
75. Uwzględniać komponent typu PROXY pośredniczący w komunikacji między serwerem SOAR a zewnętrznymi produktami działającymi w separowanych i chronionych segmentach sieci, dla realizacji ich integracji i wykonywania zadań automatyzacji.
76. Uwzględniać komponent umożliwiający separację zarówno na poziomie sieciowym jak i wykonawczym (osobny system uruchamiający skrypty) integracji wykonujących operacje niebezpieczne lub generujące ruch sieciowy postrzegany z punktu widzenia organizacji jako niebezpieczny bądź wymagający zastosowania osobnego łącza internetowego (np. wykonywanie zrzutów ekranu stron internetowych, renderowanie wiadomości email z obrazkami / załącznikami, port scanning itp.).
77. Wspierać model RBAC do zarządzania dostępem do komponentów systemu w oparciu o zasadę “the principle of minimal privileges” (https://pl.wikipedia.org/wiki/ Zasada_najmniejszego_uprzywilejowania).
78. W szczególności powinna być możliwość modyfikacji poziomu dostępu do:
    - playbook-ów,
    - skryptów automatyzacji,
    - komend w ramach danej integracji (jeśli istnieje wiele instancji tej samej integracji, można przypisać różne role (poziom uprawnień) do tej samej komendy w każdej z instancji),
    - elementów interfejsu.
79. Pozwolić na powiązanie ról w modelu RBAC z odpowiednimi obiektami w zewnętrznych systemach uwierzytelniania (ip.. powiązanie ról RBAC z rolami SAML lub grupami AD).
80. Uwzględniać możliwość definiowania zmianowości pracy analityków SOC (przykładowo w obrębie roli użytkownika systemu SOAR).
81. Zapewniać granularny poziom logowania operacji wykonanych w systemie przez użytkowników rozwiązania, w celach audytowych. Logowane powinny być co najmniej takie operacje jak:
    - logowanie do systemu,
    - tworzenie, usuwanie oraz edycja playbook-ów, skryptów a także innych obiektów w systemie,
    - instalacja nowych integracji,
    - zmiana konfiguracji rozwiązania.
82. Wykorzystywać mechanizmy uczenia maszynowe (ang. Machine Learning) celem zwiększenia efektywności oraz produktywności centrów operacji bezpieczeństwa SOC. W szczególności algorytmy uczenia maszynowego powinny wspierać analityków w zakresie:
    - sugerowania komend podczas analizy incydentu bazując na danych z historycznie rozwiązanych incydentów,

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

- przypisania analityka do incydentu bazując na aktualnym obciążeniu lub podobnych zamkniętych w przeszłości incydentach,
- podpowiedzi przy tworzeniu scenariuszy (tzw. playbooks),
- wyszukiwania powiązanych i zduplikowanych incydentów.

83. Wspierać model uczenia nadzorowanego dla najbardziej popularnych i czasochłonnych w ocenie incydentów typu phishing. SOAR na podstawie incydentów typu phishing z przeszłości, które zostały już sklasyfikowane (i rozwiązane), powinien zbudować model do automatycznej oceny nowych przychodzących wiadomości celem ich klasyfikacji jako: 'Poprawna', 'Spam' lub 'Złośliwa'.

IV. Oferowany System nie może mieć:

1. Ograniczeń licencyjnych na ilość dostępnych scenariuszy, integracji, akcji automatyzacji, liczby podłączonych konektorów, rozmiarów dysku, incydentówtp.tp.
2. Ograniczeń licencyjnych na ilość przetwarzanych informacji w ramach integracji z rozwiązaniami firm trzecich.
3. Ograniczeń licencyjnych na skalowanie systemu wszerz poprzez dodawanie pomocniczych maszyn, zrównoleglających przetwarzanie.

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