Załącznik nr 1 do Rozeznania rynku

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostarczenie, zaprojektowanie, wdrożenie, integracja, uruchomienie, utrzymanie i rozwój platformy do scentralizowanego zarządzania i automatyzacji procesów reagowania na incydenty bezpieczeństwa, wspierającej zespół analityków w obsłudze incydentów, w środowisku teleinformatycznym Zamawiającego.

Spis treści

Wprowadzenie

Celem niniejszego Zapytania jest przedstawienie wymagań i potrzeb Zamawiającego w zakresie dostarczenia, zaprojektowania, wdrożenia, integracji, uruchomienia, utrzymania i rozwoju platformy do scentralizowanego zarządzania i automatyzacji procesów reagowania na incydenty bezpieczeństwa, wspierającej zespół analityków w obsłudze incydentów, w środowisku teleinformatycznym Zamawiającego, zwanej dalej jako Platforma.

Słownik pojęć i skrótów

Pojęcie/skrót	**Wyjaśnienie**
API	Application Programming Interface. Interfejs programistyczny do udostępniania funkcjonalności systemu.
BPMN	Business Process Model and Notation. Format tworzenia schematów postępowania (flowcharts) ze szczególnym uwzględnieniem zastosowania w aspekcie cyberbezpieczeństwa.
CSIRT	Computer Security Incident Response Team. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym wg. Ustawy o Krajowym Systemie Cyberbezpieczeństwa.
CTI	Cyber Threat Intelligence. Gromadzenie, analiza i wymiana informacji o cyberzagrożeniach.
Akcja konektora, akcja	Zdefiniowane wcześniej w ramach konektora akcje, które pozwalają na wykonywanie podstawowych czynności integracyjnych. Przykładem akcji może być: aktualizacja konta użytkownika, sprawdzenie dostępnych informacji o adresie IP, etc.
Konektor	Rozszerzenie Platformy w postaci spójnej biblioteki wraz z akcjami i dokumentacją. Celem konektora jest umożliwienie współdziałania z zewnętrznymi systemami dla uzyskania dodatkowych informacji lub wykonania zmian w zewnętrznym systemie.
GUI	Graficzny interfejs użytkownika, GUI. Sposób komunikowania się człowieka z oprogramowaniem komputera, wykorzystujący obiekty wyświetlane na monitorze w trybie graficznym; do wprowadzania danych korzysta się z klawiatury i myszy.
HTTP	Hypertext Transfer Protocol. Protokół przesyłania danych hipertekstowych.
IoC	Indicator of compromise. Wskaźnik naruszenia bezpieczeństwa, określa cechy charakterystyczne i artefakty związane z incydentem bezpieczeństwa.
Incydent, Incydent bezpieczeństwa, Incydent cyberbezpieczeństwa	Zdarzenie związane z naruszeniem bezpieczeństwa.
Multitenant	Model pracy aplikacji lub systemy w trybie współdzielenia zasobów pomiędzy wielu klientów lub organizacji (tenantów). System pracujący w tym trybie kontroluje prawa każdej organizacji i zapewnia logiczną separację.
VMware	Oprogramowanie do wirtualizacji infrastruktury teleinformatycznej.
Oprogramowanie	Oprogramowanie Platformy.
Playbook	Procedura programowana w Platformie, składająca się z sekwencji działań podejmowanych przez oprogramowanie zgodnie z założonym przepływem.

Platforma	W tym przypadku rozumiana jako system informatyczny służący do scentralizowanego zarządzania i automatyzacji procesów reagowania na incydenty bezpieczeństwa, wspierającej zespół analityków w obsłudze incydentów, w środowisku teleinformatycznym Zamawiającego.
RBAC	Role-basedaccesscontrol (RBAC), kontrola dostępu oparta na rolach – mechanizm kontroli dostępu w systemach komputerowych.
SDK	SDK to zbiór oprogramowania używanego do programowania aplikacji dla określonego urządzenia lub systemu operacyjnego
SIEM	Security Information and Event Management. System do zarządzania informacją i zdarzeniami cyberbezpieczeństwa.
SOC	Security Operation Center. Zespół wykwalifikowanych specjalistów którego celem jest monitorowanie bezpieczeństwa teleinformatycznego, wykrywanie i reagowanie na Incydenty bezpieczeństwa przy wykorzystaniu zarówno środków technicznych i organizacyjnych.
Workflow	Sposób przedstawienia i organizacji przepływu informacji pomiędzy rozmaitymi obiektami biorącymi udział w jej przetwarzaniu
STIX	Structured Threat Information Expression. Format danych używany do wymiany informacji o cyberzagrożeniach.
Service Desk	System zarządzający zgłoszeniami serwisowymi.
TAXII	Trusted Automated Exchange of Intelligence Information. Protokół warstwy aplikacji służący do przekazywania informacji o cyberzagrożeniach w prosty i skalowalny sposób.
VM	Vulnerability Management. Zarządzanie wykrytymi podatnościami.

Wymagania w zakresie Platformy – warunki konieczne.

ID	Opis
1.	Wszystkie elementy Platformy MUSZĄ pochodzić od tego samego producenta oraz komunikacja użytkownika z Platformą MUSI się odbywać za pomocą pojedynczego interfejsu użytkownika.
2.	Platforma MUSI mieć możliwość instalacji w infrastrukturze Zamawiającego bez żadnego elementu wykonawczego, analitycznego lub innego znajdującego się poza infrastrukturą Zamawiającego.
3.	Platforma MUSI mieć możliwość domyślnej instalacji w środowisku wirtualizacyjnym i MUSI wspierać co najmniej środowiska producentów VMWare oraz Red Hat KVM.
4.	Platforma MUSI być dostarczona jako kompletny obraz do instalacji. Zarówno system operacyjny takiego obrazu jak i oprogramowanie muszą być utrzymywane przez producenta Platformy, tzn poprawki i aktualizacje pochodzą od producenta i są objęte jego gwarancją.
5.	Platforma MUSI posiadać licencjonowanie oparte o ilość użytkowników jednocześnie korzystających z systemu – weryfikacja powinna być realizowane w oparciu jednoczesne aktywne sesje zalogowanych użytkowników.
6.	Platforma NIE MOŻE licencjonować lub ograniczać innych parametrów systemu, jak ilość wykonywanych akcji, liczba podłączonych konektorów, rozmiar dysku, itp.
7.	Platforma MUSI mieć możliwość obsługi wielu organizacji w ramach jednej instalacji (*multitenant*). Informacje w ramach jednej organizacji MUSZĄ być odseparowane od pozostałych w ramach interfejsu i ról operatora.
8.	Platforma MUSI mieć możliwość wyboru wielu języków interfejsu graficznego GUI. Musi istnieć możliwość zaimplementowania języka polskiego.
9.	Platforma MUSI mieć możliwość pracy hybrydowej dla trybu obsługi wielu organizacji (*multitenant*), tzn. musi istnieć możliwość komunikacji z/do podległej organizacji zarówno bezpośrednio z centralnego systemu jak i lokalnie zainstalowanego systemu w obsługiwanej organizacji, który jest dedykowanym i wydzielonym elementem.
10.	W ramach trybu obsługi wielu organizacji (*multitenant*) MUSI istnieć możliwość licencjonowania i tworzenia dedykowanych kont operatorów w ramach danej organizacji, którzy mają dostęp do danych tylko i wyłącznie w swoim zakresie.
11.	Platforma MUSI mieć możliwość instalacji oraz aktualizacji w trybie offline, tzn. bez dostępu do Internetu. Wymaganie dotyczy również pracy z konektorami.
12.	Producent Platformy MUSI dostarczać aktualizacje obejmujące zarówno system operacyjny jak i oprogramowanie Platformy.
13.	Aktualizacja konektorów NIE MOŻE powodować restartu systemu.
14.	Aktualizacja istniejących konektorów i obsługiwanych przez producenta MUSI być realizowana z poziomu GUI, bez konieczności uruchamiania innego interfejsu. Aktualizacje MUSZĄ być widoczne w interfejsie Platformy od momentu ich dostępności (dotyczy pracy w trybie online).
15.	Platforma MUSI zawierać kreator wspomagający tworzenie niestandardowych integracji. Jednocześnie wszystkie istniejące integracje (konektory i ich akcje) muszą być edytowalne za pośrednictwem GUI, wraz z możliwością pracy nad kodem źródłowym, bez konieczności używania zewnętrznego IDE.
16.	Konektory MUSZĄ posiadać funkcję automatycznej weryfikacji działania, tzn. muszą weryfikować poprawność ustawień i prawidłową współpracę z systemem integrowanym poprzez wykonywania aktywnych testów połączenia. Wynik weryfikacji MUSI być widoczny, a błędy muszą być logowane.
17.	Wszystkie konektory MUSZĄ udostępniać swój kod źródłowy dla administratora Zamawiającego z poziomu systemu. MUSI też być możliwa swobodna modyfikacja kodu oraz wersjonowanie konektora. MUSI być możliwość dodawania własnych akcji w ramach danego pakietu.

18.	Jeśli system, z którym łączy się Platforma dopuszcza połączenie szyfrowane, np. poprzez protokół SSL i weryfikację certyfikatu, to połączenie takie MUSI być zrealizowane w taki sposób przez Platformę
19.	MUSI istnieć możliwość pisania własnych konektorów w języku python. Proces tworzenia nowego konektora MUSI być możliwy do realizacji w środowisku zewnętrznym jak i w ramach zainstalowanego systemu. Platforma MUSI posiadać możliwość importu konektorów z przygotowanego wcześniej archiwum.
20.	Producent MUSI dostarczyć zestaw bibliotek SDK dla łatwego tworzenia własnych konektorów.
21.	Platforma MUSI posiadać publicznie dostępne repozytorium dla integracji, konektorów, pakietów rozszerzeń np. github. Repozytorium to MUSI być aktualizowane zarówno przez producenta jak i społeczność użytkowników.
22.	Platforma MUSI posiadać publicznie dostępną dokumentację co najmniej w zakresie: instalacji i pierwszej konfiguracji, dokumentacji dla dostępnych w systemie konektorów, API, administracji systemem, ścieżki aktualizacji wersji, informacji o wydaniu (release notes), tworzenie konektorów oraz Playbook-ów.
23.	Producent Platformy MUSI utrzymywać dedykowany (odrębny od wspomnianej dokumentacji) portal dla treści związanych z konfiguracją systemu obejmujący co najmniej: konektory, gotowe szablony konfiguracji, elementy interfejsu graficznego. Portal ten musi pozwalać na pobieranie wcześniej wymienionych, gotowych do importu modułów. Portal MUSI być dostępny publicznie i NIE MOŻE wymagać jakichkolwiek opłat za korzystanie z zawartości i nie może wymagać zakładania konta celem dostępu do treści.
24.	Zamawiający wymaga, aby oferowana Platforma dostarczona była również w wersji testowej. Wersja testowa MUSI posiadać taką samą funkcjonalność i wersję jak produkcyjna. MUSI być możliwe uruchomienie więcej niż jednej instancji testowej.
25.	Platforma MUSI umożliwiać importowanie części konfiguracji lub interfejsu z innego systemu, np. testowego.
26.	Interfejs graficzny MUSI udostępniać szatę kolorystyczną GUI co najmniej w jasnych barwach i ciemnych (darkmode).
27.	Platforma MUSI posiadać elastyczną możliwość integracji z zewnętrznymi systemami, najlepiej w formie konektorów, za pomocą dostępnych protokołów, nie mniej niż: API, SSH, Syslog, TAXII, SMTP, SOAP, IMAP, bazy danych, pliki w formatach XML, HTML i JSON, SMB, LDAP, SSL. Dla każdego integrowanego producenta MUSZĄ być dostępne akcje charakterystyczne dla danego rozwiązania. MUSI być możliwość instalacji tylko niezbędnych do działania konektorów.
28.	Platforma MUSI posiadać graficzny interfejs budowania i symulacji Playbook-ów.
29.	Edytor Playbook-ów MUSI udostępniać co najmniej następujące typy elementów wykonawczych: 1. Wykonanie zadania przez użytkownika technicznego (personel SOC/CSIRT) 2. Wykonanie zadania przez użytkownika biznesowego 3. Wykonanie automatycznego zadania w zintegrowanym z Platformą systemie bezpieczeństwa Zamawiającego 4. Wykonanie automatycznego zadania w elemencie infrastruktury teleinformatycznej Zamawiającego
30.	Projektowanie i wykonywanie Playbook-ów MUSI udostępniać możliwość złożonych ścieżek postępowania, w tym co najmniej: 1. Ścieżek równoległych 2. Ścieżek alternatywnych 3. Ścieżek warunkowych
31.	Playbook MUSI udostępniać możliwość budowania rozdzielnych ścieżek postępowania na każdym jego etapie w zależności od parametrów wejściowych dodanego elementu.
32.	Wykonywanie Playbook-ów MUSI udostępniać możliwość: 1. Rozwidlania na wiele ścieżek

	2. Zbieżności wielu ścieżek w jednym elemencie
33.	Platforma MUSI udostępniać możliwość budowania nowych Playbook-ów na bazie już istniejących poprzez kopiowanie i edycję.
34.	Platforma MUSI udostępniać możliwość wersjonowania Playbook-ów.
35.	Platforma MUSI posiadać możliwość importu do Playbook-ów workflow z narzędzia BPMN. MUSI być obsługiwany format pliku źródłowego XML i JSON.
36.	Platforma MUSI umożliwiać tworzenie Playbook-ów zagnieżdżonych tzn. korzystających z już istniejących, gdzie istniejący Playbook jest częścią utworzonego nowego playbook-a.
37.	Platforma MUSI posiadać mechanizmy wyboru ścieżki/ścieżek w Playbook-ach na podstawie kontekstu danych/parametrów.
38.	Platforma MUSI się integrować z zewnętrznymi systemami CTI (Cyber Threat Intelligence).
39.	Platforma MUSI posiadać warstwowy mechanizm przetwarzania obsługiwanych alarmów. Minimalny zakres to: stopień 1: przetwarzanie odebranych rekordów z zewnątrz zanim zostanie on zapisany w systemowych bazach danych (możliwe jest na przykład odrzucenie rekordu do dalszego przetwarzania); stopień 2: właściwe przetwarzanie procedur; stopień 3: działania po wykonaniu procedur (playbook), przez co możliwe jest na przykład zaawansowane łączenie podobnych rekordów z nowo utworzonym.
40.	Producent Platformy MUSI dostarczać własną bazę CTI (Cyber Threat Intelligence) możliwą do uruchomienia w systemie oraz zapewnić jej aktualizacje nie rzadziej niż 1 raz na dobę.
41.	Platforma MUSI posiadać interfejsy pozwalające na integrację z rozwiązaniami CyberThreat Intelligence firm trzecich (STIX, TAXII).
42.	Integracja z CTI MUSI umożliwiać pobieranie przez Platformę 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.).
43.	Platforma MUSI posiadać możliwość wprowadzania informacji o Incydentach różnymi interfejsami w tym co najmniej: 1. Poprzez Operatora manualnie 2. Poprzez integracje z systemem ServiceDesk (zdarzenie zakwalifikowane jako Incydent cyberbezpieczeństwa) 3. Poprzez integracje z systemami bezpieczeństwa 4. Przez SIEM 5. Porzez pocztę elektroniczną – dedykowane konto dla powiadomień
44.	Platforma 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
45.	Platforma MUSI mieć możliwość dowolnego definiowania nowych typów artefaktów.
46.	Platforma MUSI mieć możliwość tworzenia skryptów w co najmniej języku programowania PYTHON.
47.	Platforma MUSI mieć domyślnie zdefiniowane co najmniej 5 stopni istotności Incydentów. Ilość stopni jak i ich nazwy POWINNY udostępniać możliwość definiowania.

48.	Platforma MUSI mieć możliwość TAG-owania zdarzeń, alertów, zadań i incydentów.
49.	Platforma MUSI mieć możliwość definiowania SLA na poziomie: 1. Alarmów 2. Incydentów
50.	Platforma MUSI mieć możliwość definiowania ról w zakresie rozwiązywania, zarządzania i raportowania incydentów bezpieczeństwa.
51.	Platforma MUSI mieć możliwość definiowania co najmniej pięciu rodzajów ról ze względu na uprawnienia: 1. Menadżer Incydentów 2. Pracownik I linii SOC 3. Pracownik II linii SOC 4. Pracownik III linii SOC 5. Użytkownik biznesowy
52.	Platforma MUSI posiadać możliwość integracji z systemami SIEM w zakresie przekazywania informacji o Incydentach.
53.	Platforma MUSI mieć możliwość załączania plików.
54.	Platforma MUSI mieć możliwość zamieszczania komentarzy w zadaniach.
55.	Platforma MUSI mieć możliwość cyklicznego uruchamiania Playbook-ów według ustalonego harmonogramu.
56.	Platforma MUSI umożliwiać przechowywanie danych o Incydentach z pełną informacją o operacjach wykonanych w systemie w zadanym okresie czasu.
	Platforma MUSI zawierać moduł zarządzania kryzysowego w postaci tzw. War Room, aby umożliwić współpracę między zespołami w wypadku wystąpienia krytycznych incydentów. War Room MUSI być tworzony ręcznie lub poprzez eskalację istniejącego incydentu.
57.	Moduł War Room MUSI zapewniać interfejs agregujący całościową informację o rozwiązywanym incydencie szczególnej wagi w tym: 1. Status incydentu 2. Listę aktualnie wykonywanych zadań 3. Wyniki wykonanych zadań 4. Raport aktualnej sytuacji oraz plan kolejnych działań
58.	Platforma MUSI mieć możliwość personalizowania widoków w interfejsach dla użytkowników.
59.	Platforma MUSI posiadać gotowe mechanizmy integracji z systemami bezpieczeństwa oraz infrastrukturą teleinformatyczną Zamawiającego. Lista niezbędnych integracji zostanie udostępniona po podpisaniu NDA
60.	Platforma MUSI mieć możliwość definiowania cyklicznego generowania raportów.
61.	Platforma MUSI posiadać mechanizmy logowania zdarzeń i operacji wykonywanych przez użytkownika.
62.	Platforma MUSI posiadać mechanizmy uwierzytelniania w oparciu o Active Directory i protokół SAML.
63.	Zarządzanie uprawnieniami MUSI być oparte o role.
64.	Platforma MUSI posiadać mechanizmy uwierzytelnia wieloskładnikowego.
65.	Platforma MUSI posiadać mechanizmy integracji z systemami typu PAM (ang: privileged access management).
66.	Platforma MUSI posiadać interfejs użytkownika udostępniany poprzez https.
67.	Platforma MUSI mieć możliwość automatycznego powiązania i grupowania podobnych incydentów (np. ten sam docelowy adres IP, usługa itp.)
68.	Platforma MUSI posiadać wbudowaną funkcjonalność tworzenia i zarządzania zadaniami.
69.	Wszystkie atrybuty widoku alarmów, takie jak nazwa, ważność, itp. MUSZĄ być konfigurowalne, aby użytkownicy mogli je dodawać lub usuwać z interfejsu. Ponadto MUSI istnieć możliwość tworzenia, modyfikowania i usuwania własnych niestandardowych atrybutów w dowolnym module systemu.

70.	Platforma MUSI umożliwiać skorelowanie i powiązanie rekordu typu alert, incydent, IoC z innym rekordem w systemie, w tym z niestandardowymi typami rekordów, które użytkownicy sami definiują. Relacje MUSZĄ obejmować co najmniej modele: 1. Wiele-do-wiele 2. Wiele-do-jednego
71.	Platforma MUSI mieć silnik przewidywania oparty na uczeniu maszynowym, który przewiduje wartości pól na podstawie danych historycznych. Zakres przewidywania uczenia maszynowego MUSI obejmować wszystkie moduły produktu: wbudowane (takie jak alerty, incydenty, wskaźniki, itd.) jak i niestandardowe.
72.	Widok każdego modułu GUI MUSI być dowolnie konfigurowalny za pomocą szablonu widoku, który definiuje położenie każdego pola i widżetu.
73.	Platforma MUSI zapewniać funkcję globalnego wyszukiwania, która umożliwia analitykowi wyszukiwanie poprzez słowa kluczowe w całym systemie i we wszystkich modułach.
74.	Interfejs użytkownika GUI MUSI oferować możliwość łączenia różnych rekordów razem (linkowanie). Rekordy mogą być między innymi: artefakty, zadania, War Room, użytkownicy, kampanie, assety, alarmy, załączniki, wiadomości e-mail, incydenty.
75.	MUSI być możliwa eskalacja zgłoszenia ręcznie przez operatora lub automatycznie za pośrednictwem automatycznie uruchamianego Playbook-a, który może zastosować dowolną logikę jako warunek przed wykonaniem eskalacji zgłoszenia.
76.	Incydenty, alarmy, artefakty, załączniki i moduły niestandardowe MUSZĄ udostępniać analitykom możliwość komunikowania się za pomocą komentarzy. Każda wiadomość wpisana przez analityka lub Playbook MUSI pozostać atrybutem rekordu, w którym został utworzony. Dodatkowo komentarze muszą umożliwiać: 1. tworzenie ich prostym tekstem lub tekstem sformatowanym 2. oznaczanie analityków w samym komentarzu, celem zwrócenia ich uwagi poprzez sposób typowy dla komunikatorów: @<nazwa konta> 3. uruchamianie akcji 4. obsługę tag-ów 5. obsługę załączania plików 6. zarządzanie dostępem do nich w oparciu o RBAC
77.	Platforma MUSI umożliwiać analitykowi analizę graficzną powiązań pomiędzy Incydentami i IOC. Graficzna korelacja MUSI być dostępna dla różnych typów rekordów np. assety, podatności, alarmy, incydenty.
78.	Platforma MUSI być zintegrowana z MITRE ATTACK, przez którą to możliwe będzie wzbogacenie analizy incydentów o informacje takie jak: taktyki, analiza zagrożenia i sugestie dotyczące środków zaradczych.
79.	Platforma MUSI umożliwiać skonfigurowanie obowiązkowego uzupełnienia notatek przez operatora przed zamknięciem dochodzenia, dla incydentu obejmującego co najmniej sekcje: • informacja podsumowująca • następne kroki • opis sposobu rozwiązania problemu Każde pole MUSI mieć możliwość wyboru konfiguracji: nieobowiązkowe, obowiązkowe, warunkowo obowiązkowe.
80.	Obsługa incydentów MUSI wspierać oznaczanie fazy analizowanego ataku (kill chain phase). MUSI być możliwa zmiana definicji faz jak i ich ilości. Ustawiona faza w ramach incydentu POWINNA być reprezentowana graficznie.
81.	Platforma MUSI mieć konfigurowalną funkcję zarządzania kolejkami obsługującą automatyczne przypisywanie alertów/incydentów/zadań do różnych grup obsługujących.
82.	Platforma MUSI wyodrębnić artefakty (IP, URL, Domena, itp) z ponad 1500 typów plików takich jak MS Office, PDF, itd. Wyodrębnione artefakty muszą być połączone z rekordem pliku, z którego zostały wyodrębnione. MUSI być możliwe wstępne przeglądanie wyniku analizy (preview) w postaci tekstu lub HTML.

83.	Platforma MUSI umożliwiać operatorowi edycję dostępnych pól bezpośrednio w interfejsie WebUI zgodnie z przydzielonymi uprawnieniami. Uprawnienia MUSZĄ być konfigurowalne indywidualnie dla każdego pola. Minimalny zakres uprawnień to: brak, odczyt, odczyt-zapis. Zmiany w polach MUSZĄ być widoczne w logu audytowym systemu.
84.	Playbook- i MUSZĄ być pogrupowane w foldery z możliwością eksportowania lub importowania całego folderu bezpośrednio z WebUI. Dzięki temu możliwa będzie migracja schematów pomiędzy systemem testowym a produkcyjnym.
85.	Playbook-i MUSZĄ mieć co najmniej 3 priorytety wykonywania, pozwalające na wykonanie niektórych przed innymi w kolejce w zależności od ich ważności.
86.	Playbook-i MUSZĄ mieć wyzwalanie warunkowe. Nie będą się uruchamiać, chyba że spełnione są określone warunki. Poniższe operatory warunków muszą być obsługiwane: 1. równy 2. nie równa się 3. mniej niż/mniej niż lub równa się 4. większe niż/większe niż lub równe 5. jest na liście 6. nie ma na liście 7. pusty 8. jest zgodny z zadanym wzorcem (pattern) 9. nie jest zgodny z zadanym wzorcem (pattern) Warunki MUSZĄ obsługiwać sumę logiczną (dowolny warunek spełniony) oraz iloczyn logiczny (wszystkie warunki muszą być spełnione).
87.	Playbook-i MUSZĄ obsługiwać następujące sposoby uruchomienia: • analityk może ręcznie uruchomić w GUI systemowym • automatycznie przy zmianie rekordu (Alert, wskaźnik, incydent... itd.): utworzony/zmieniony/usunięty • przez API: gdy Platforma otrzyma żądanie API z określonymi parametrami to uruchamia określonego Playbook-a • referencja: playbook ma możliwość wykonania innego playbook-a z zadanymi parametrami
88.	Platforma MUSI zapewniać graficzny edytor Playbook-ów, w którym użytkownicy mogą używać myszy do przeciągania i upuszczania operacji lub kolejnych kroków. Ponadto edytor playbook MUSI zawierać panele pomocnicze do pobierania wszystkich dostępnych zmiennych, wybierania wszystkich typów operacji, tworzenia wyrażeń złożonych. Tworzenie Playbook-a lub jego edycja NIE MOŻE wymagać uruchamiania jakiegokolwiek innego interfejsu.
89.	Graficzny edytor Playbook-ów MUSI mieć możliwość cofania kroków edycji jak i ich ponawiania. Przykładowo możliwe jest przywrócenie wcześniej usuniętej operacji.
90.	Platforma MUSI umożliwiać użytkownikowi uruchomienie Playbook-a z poziomu edytora graficznego i przetestowanie jego wykonania z zmiennymi wybranego rekordu istniejącego w systemie lub ostatnim rekordem, z którym Playbook został wykonany.
91.	Administratorzy muszą mieć możliwość indywidualnego eksportowania i importowania Playbook-ów, w tym dowolnie wybranej wersji (podobnie jak SVN / GIT).
92.	Platforma MUSI obsługiwać tworzenie, modyfikowanie i usuwanie zmiennych globalnych dostępnych dla wszystkich Playbook-ów. Zmienne globalne muszą być edytowalne za pomocą Playbook-ów lub GUI.
93.	Platforma MUSI dostarczyć wizualną historię wykonania Playbook-ów, która identyfikuje dane wyjściowe, wejściowe i konfigurację każdego kroku.
94.	Poziom logowania wykonywania Playbook-ów MUSI być konfigurowalny zarówno globalnie (w całym systemie) jak i lokalnie dla każdego Playbook-a indywidualnie. Muszą być wspierane co najmniej dwa poziomy logowania: informacyjny i debug.

<table>
<tr><td>95.</td><td>Narzędzia do debugowania muszą być dostępne z poziomu edytora Playbook-ów. Debugger MUSI być w stanie korzystać z danych z poprzedniego wykonania Playbook-a lub danych dostarczonych przez analityka.</td></tr>
<tr><td>96.</td><td>Kontrola praw dostępu (RBAC) MUSI obejmować Playbook-i w zakresie zapisu i uruchamiania.</td></tr>
<tr><td>97.</td><td>Platforma MUSI zawierać szczegółowe komunikaty o błędach, gdy wykonanie Playbook -a nie powiedzie się i zezwalać na ponowne uruchomienie Playbook-a od kroku, w którym wykonanie nie powiodło się.</td></tr>
<tr><td>98.</td><td>Kroki warunkowe w wykonywaniu Playbook-ów muszą być wystarczająco elastyczne, aby móc stosować złożone warunki. Wymagane możliwości budowania warunków:
<table>
<tr><td>równy</td><td>porównuje dwa obiekty i wykonuje operację, gdy równe</td></tr>
<tr><td>nierówna się</td><td>porównuje dwa obiekty i wykonuje operację, gdy nie równe</td></tr>
<tr><td>większy niż</td><td>prawda, jeśli lewa strona jest większa niż prawa strona</td></tr>
<tr><td>większy niż lub równy</td><td>prawda, jeśli lewa strona jest większa lub równa prawej stronie</td></tr>
<tr><td>mniejsze niż</td><td>prawda, jeśli lewa strona jest mniejsza niż prawa strona</td></tr>
<tr><td>mniejsze lub równe</td><td>prawda, jeśli lewa strona jest mniejsza lub równa prawej stronie</td></tr>
<tr><td>i</td><td>zwróć wartość „prawda”, jeśli lewe i prawe wyrażenie są prawdziwe</td></tr>
<tr><td>lub</td><td>zwróć wartość „prawda”, jeśli lewe lub prawe wyraże nie jest prawdziwe</td></tr>
<tr><td>nie</td><td>negacja</td></tr>
<tr><td>dodawanie</td><td>dodaje do siebie dwa obiekty</td></tr>
<tr><td>odejmowanie</td><td>odejmij drugą liczbę od pierwszej</td></tr>
<tr><td>dzielenie</td><td>dzielenie dwóch liczb</td></tr>
<tr><td>modulo</td><td>obliczanie reszty z dzielenia liczby całkowitej</td></tr>
<tr><td>mnożenie</td><td>mnożenie dwóch wartości</td></tr>
<tr><td>potęga</td><td>podnieś lewy operand do potęgi prawego operandu</td></tr>
</table>

Warunki takie jak:
(zmienna_X + zmienna_Y)/2 > 3
((zmienna_X + zmienna_Y)/2 >zmienna_Z) OR (zmienna_A / zmienna_B) < 2
muszą być możliwe bez użycia języka programowania .Etap podejmowania decyzji MUSI mieć opcję ustawienia domyślnego następnego kroku, jeśli wszystkie warunki zawiodą.</td></tr>
<tr><td>99.</td><td>Operatorzy muszą mieć możliwość zastosowania języka programowania, co najmniej Python bezpośrednio w Playbook-ach. Administrator Platformy MUSI być w stanie ograniczyć dostęp i możliwość wykorzystania bibliotek języka python (z dokładnością do pojedynczych bibliotek).</td></tr>
<tr><td>100</td><td>Kroki Playbook-ów muszą być konfigurowalne na wypadek wystąpienia błędu. Jeśli wystąpi błąd na poziomie kroku to MUSI być możliwy wybór co najmniej przekazania komunikatu o błędzie do następnego kroku i kontynuowanie lub zaprzestanie dalszego wykonywania.</td></tr>
<tr><td>101</td><td>Zarządzanie Playbook-ami MUSI umożliwiać analitykom zbiorczą ich edycję z możliwością wykonywania poniższych funkcji:
1. Zmiana statusu (Playbook aktywny lub nieaktywowany)
2. Klonowanie wybranych Playbook-ów
3. Przenoszenie wybranych Playbook-ów do innej grupy
4. Zmiana poziomu logowania dla wybranych Playbook-ów
5. Eksportowanie wybranych Playbook-ów</td></tr>
</table>

102	Każdy Playbook w ramach proponowanego rozwiązania MUSI mieć możliwość automatycznego uruchomienia w określonych odstępach czasu z możliwością zapobieżenia jego wykonaniu, jeśli poprzednie wystąpienie jest nadal uruchomione.
103	W ramach edytora Playbook-ów analitycy muszą być w stanie wykonać operacje: • sklonuj krok • kopiuj i wklej krok lub grupę kroków do tego samego Playbook-a lub innego • wyrównaj wizualnie kroki na diagramie do układu pionowego lub poziomego - wybierz krok lub grupę kroków i usuń je
104	Playbook-i MUSZĄ mieć możliwość wykonania kroku, gdzie konfigurowalne będzie uzyskanie danych i/lub potwierdzenia za pośrednictwem wiadomości e-mail zawierającej link do decyzji z opcją podjęcia określonej akcji w przypadku przekroczenia limitu czasu. Przykładem może być wysłanie wiadomości z prośbą o zgodę na restart urządzenia wraz z informacją zwrotną o dogodnym terminie.
105	Platforma MUSI zapewniać przyjazny dla użytkownika kreator pozyskiwania danych zewnętrznych (np. informacje o użytkownikach, podatnościach) w celu stworzenia mechanizmu integracji pozwalającego na ciągłe i automatyczne pobierania wymaganych informacji..
106	Platforma MUSI zapewnić pulpit (dashboard) z informacją o kondycji konektorów, który wskazuje, czy wszystkie integracje z systemami zewnętrznymi działają prawidłowo.
107	Akcje konektorów muszą podlegać prawom dostępu RBAC tak aby tylko zdefiniowane role mogły używać zdefiniowanych akcji z dokładnością do pojedynczej akcji.
108	Platforma MUSI umożliwiać analitykowi uruchamianie dowolnej akcji konektora do której ma prawo, za pośrednictwem interfejsu GUI bez użycia Playbook-a.
109	Musi istnieć możliwość zbiorczego importu i eksportu wskaźników IOC bezpośrednio z GUI.
110	Platforma MUSI być na tyle elastyczna, aby umożliwić generowanie reputacji wskaźników na podstawie danych z różnych źródeł Threat Intelligence jednocześnie.
111	Platforma MUSI umożliwiać tworzenie kopii zapasowych i przywracanie zarówno konfiguracji systemu, jak i zebranych danych.
112	Platforma MUSI mieć możliwość tworzenia niestandardowych modułów funkcjonalnych z poziomu interfejsu GUI. Moduł jest podsystemem do zarządzania nowym typem rekordów, takich jak: Alerty, Incydenty, wskaźniki, itp.
113	Architektura Platformy MUSI pozwalać na skalowanie rozwiązania jak i tworzenie wysokiej dostępności. Musi istnieć możliwość klastrowania wielu węzłów (minimum 3) w konfiguracji Aktywny/Aktywny.
114	Platforma MUSI oferować skalowalną geograficznie, rozproszoną architekturę z możliwością separacji części zasobów dla podległych jednostek lub innych użytkowników (model pracy MSSP).
115	Platforma MUSI umożliwiać uruchamianie Playbook-ów i kolekcję danych w zdalnych segmentach sieci za pośrednictwem agenta wdrożonego w segmencie sieci zdalnej. Agenty muszą obsługiwać automatyczne aktualizacje.
116	Platforma MUSI umożliwiać korzystanie zarówno z wewnętrznej, jak i zewnętrznej bazy danych.
117	Platforma MUSI oferować aplikację mobilną co najmniej dla systemu Android do zdalnego zarządzania i monitorowania w ramach Platformy.
118	Platforma MUSI zapewniać globalne logowanie aktywności (audyt) obejmujące zarówno działania użytkowników (takie jak logowanie, wylogowanie, instalacje, itp.) jak i zdarzenia związane z danymi (np tworzenie rekordów, aktualizowanie, usuwanie...)
119	Platforma MUSI mieć możliwość przesyłania zdarzeń audytu i aplikacji do serwera zewnętrznego lub rozwiązania SIEM. Następujące protokoły muszą być obsługiwane z konfigurowalnym poziomem dziennika: 1. UDP 2. TCP, TCP/TLS 3. RELP, RELP/TLS

120	Platforma MUSI posiadać skonfigurowany widżet osi czasu dziennika inspekcji śledzący każde zdarzenie dla rekordu w alarmach, incydentach ze szczegółami każdej zmiany. Przykłady: uruchomienie Playbook-a, dodanie komentarza, zmiana wartości, etc.
121	Platforma MUSI zapewniać szczegółową i elastyczną kontrolę dostępu opartą na rolach (RBAC). Administratorzy muszą mieć możliwość ustawienia praw dostępu dla każdego typu rekordu do poziomu pola. Na przykład pole „źródłowy adres IP”.
122	Platforma MUSI obsługiwać hierarchię grup użytkowników. Grupa MUSI mieć możliwość dziedziczenia zakresu dostępu z innej grupy lub grup według poziomów: grupa nadrzędna (parent) – ma dostęp do danych niższych grup i swojej • grupa równoważna (sibling) – ma dostęp do danych grup w ramach ustawionego połączenia • grupa podrzędna (child) – brak możliwości dostępu do danych z nadrzędnych grup
123	Platforma MUSI zapewniać wiele konfigurowalnych pulpitów nawigacyjnych (dashboard), które działają zgodnie z prawami dostępu RBAC.
124	Platforma MUSI zapewniać mechanizm wyróżniania alertów, które zbliżają się do naruszeń SLA.
125	Pulpit nawigacyjny MUSI móc wyświetlać informacje specyficzne dla analityka, takie jak alerty i zadania przypisane do niego.
126	MUSI być możliwe importowanie i eksportowanie szablonów pulpitu nawigacyjnego.
127	Platforma MUSI posiadać skonfigurowane pulpity nawigacyjne dedykowane dla ról, takich jak: analityk linii 1, analityk linii 2, menedżer SOC.
128	Platforma MUSI mierzyć wskaźniki SOC dla incydentów, takie jak średni czas dla poszczególnych faz ataku wg. killchain. Powinno być możliwe wyświetlanie tych danych na pulpicie nawigacyjnym.
129	Platforma MUSI mieć dedykowany pulpit nawigacyjny do monitorowania stanu/dostępności każdej integracji, a także kondycji Platformy.
130	Platforma MUSI obsługiwać dostosowanie znaków graficznych (branding) interfejsu użytkownika dla różnych domen MSSP.
131	Platforma MUSI zapewniać framework dla przygotowana własnego pulpitu nawigacyjnego zgodny z HTML/JSON/JS, aby umożliwić tworzenie niestandardowych widżetów pulpitu nawigacyjnego i importowanie ich do Platformyy.
132	Platforma MUSI zapewniać w dostępnym dla użytkownika interfejsie graficznym, konfigurowalny moduł raportowania.
133	Raporty MUSZĄ mieć możliwość zaplanowania uruchamiania w czasie zdefiniowanym przez użytkownika.
134	Raporty MUSZĄ być generowane w co najmniej formatach CSV i PDF.
135	Wygenerowane raporty MUSZĄ mieć opcję wysłania pocztą elektroniczną.
136	MUSI być możliwe uruchamianie raportów z poziomu playbook.
137	Dostęp do raportów MUSI być ograniczany prawami dostępu RBAC.
138	Platforma MUSI posiadać logi audytu, które dostarczą informacji o aktywności modułu raportowego, włączając akcję pobrania raportu.
139	MUSI istnieć możliwość dołączania do raportu grafik i wykresów.
140	Platforma MUSI posiadać moduł zarządzania zmianą operatorów, w szczególności MUSZĄ być obsługiwane funkcje: 1. generowanie kalendarza zmiany wg założonego wzoru, np. 8 godzin od 6:00 na tydzień do przodu, dni robocze dla wybranych użytkowników 2. przekazywanie zmiany: przydzielanie niezamkniętych dochodzeń zmiany kończącej do zmiany rozpoczynającej pracę 3. przypisywanie musi być możliwe dla wszystkich niezamkniętych spraw, które rozpoczęły się w zadanym przedziale czasu, np. ostatnie 7 dni 4. przypisywane rekordy muszą mieć możliwość filtrowania:

	o filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne) o poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione) 5. musi być możliwe przypisanie rekordu: o nie przypisany o przypisany kierownikowi zmiany o wg. metody round robin w ramach członków zmiany
141	Platforma MUSI posiadać moduł zarządzania kolejkami nadchodzących zdarzeń. Domyślnie musi być możliwe tworzenie dedykowanych kolejek dla rekordów typu zadanie, alarm i incydent. Każda kolejka musi się charakteryzować funkcjami co najmniej: 1. wybór typu rekordu – dowolny zestaw (jeden typ, wszystkie typy) 2. musi być możliwe dodawanie nowych typów rekordów do kolejek 3. kolejka musi obsługiwać filtry wejściowe dla rekordów, minimalny zakres to: o utworzenie lub aktualizacja rekordu o filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne o poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione) 4. musi być możliwe ustawienie priorytetu rekordu w ramach kolei 5. musi być możliwe przypisanie rekordu: o nie przypisany o przypisany kierownikowi grupy o wg. metody roundrobin w ramach członków grupy

Wymagania w zakresie Platformy – warunki opcjonalne.

ID	Opis
1	Platforma jest licencjonowana w modelu licencji wieczystych. Dostawca dostarczy licencje na czas nieoznaczony, wraz ze wsparciem producenta na okres 36 miesięcy.
2	Platforma umożliwia wybór przydziału licencji dla użytkowników, według następującego sposobu: a) przypisywania licencji na sesję dla kont imiennych, gdzie jedno konto zużywa jedną licencję b) tworzenie kont wspólnych, które działają w ramach pozostałej puli dostępnych połączeń. Zmiana trybu licencji dla poszczególnych kont jest możliwa w dowolnym momencie.

Wymagania w zakresie usług

Zakres projektu

1.a. Analiza przedwdrożeniowa środowiska bezpieczeństwa.

Zamawiający wymaga gruntownej analizy przedwdrożeniowej obejmującej implementację Platformy w infrastrukturze Zamawiającego oraz zaproponowanie optymalnego sposobu wdrożenia Platformy.

Wynikiem analizy będzie dokument opisujący co najmniej:

- obecną architekturę środowiska bezpieczeństwa Zamawiającego

- rozwiązania bezpieczeństwa wykorzystywane przez Zamawiającego

- funkcjonalności istniejące w ekosystemie bezpieczeństwa Zamawiającego, aktualnie wykorzystywane i możliwe do stosowania w przyszłości

1. b. Analiza przedwdrożeniowa procesów reakcji na incydent bezpieczeństwa.

Zamawiający wymaga analizy procesów reakcji na incydenty bezpieczeństwa oraz szczegółowych procedur reakcji na wystąpienie incydentu (60 playbooków). Analiza powinna zawierać utworzenie modelu ryzyk i zagrożeń zgodnie ze standardami NIST SP 800-30 rev. 1 zał D, SP 800-53 rev. 5, analizę stopnia pokrycia przez istniejące procesy, procedury, sposoby detekcji i mitygacji, zgodnie z CSF 2.0, SIM3 oraz wskazanie obszarów do poprawy.

Wynikiem analizy będzie:

- model ryzyk i zagrożeń

- ocena zgodności z SIM3

- stopień pokrycia zgodnie z CSF 2.0

2. Dostawa licencji.

Dostawa licencji Platformy zgodnie z SWZ wraz ze wsparciem producenta na okres 36 miesięcy licząc od daty dostawy Platformy. Licencje powinny umożliwiać jednoczesną pracę w systemie dla min. 15 użytkowników Zamawiającego dla środowiska produkcyjnego i min. 2 użytkowników dla środowiska testowego.

Platforma musi spełniać założenia opisane w SWZ.

3. Wdrożenie.

Zakres wdrożenia.

1. Przygotowanie przez Wykonawcę dokumentacji przedwdrożeniowej w postaci co najmniej projektu technicznego oraz harmonogramu wdrożenia.
2. Dostarczenie, instalacja i konfiguracja systemu w infrastrukturze posiadanej przez Zamawiającego;

3. Integracja z systemami bezpieczeństwa Zamawiającego:
    a. bramka pocztowa,
    b. exchange,
    c. firewalle,
    d. SIEM
    e. IDS,
    f. AD,
    g. proxy,
    h. EDR,
    i. DLP,
    j. skanery podatności
4. Integracja z zewnętrznymi źródłami danych o zagrożeniach, wskazanymi przez Zamawiającego – do 10 źródeł w ramach projektu wdrożenia.
5. Zaprojektowanie co najmniej 10 playbooków, automatyzujących pracę Działu SOC. Prace powinny być wykonane w oparciu o wcześniej przeprowadzoną przez Dostawcę analizy przedwdrożeniowe (analiza środowiska bezpieczeństwa, analiza procesów reakcji na incydenty bezpieczeństwa) i best practise.
6. Implementacja co najmniej 10 playbooków na podstawie opracowanych wspólnie przez Zamawiającego i Wykonawcę dokumentów;
7. Testy poprawności działania całego rozwiązania;
8. Przygotowanie dokumentacji powdrożeniowej.
9. Szkolenia dla operatorów - dla max. 30 osób (3 grupy po 10 osób);
   Szkolenia będą prowadzone w siedzibie Zamawiającego w Warszawie lub w formule zdalnej, w wymiarze do 6 godzin dla każdej z grup.

4. Wsparcie powdrożeniowe Wykonawcy przez okres 36 miesięcy.

1. Wsparcie serwisowe Wykonawcy, świadczone przez inżynierów w języku polskim dla dostarczonej i wdrożonej Platformy, przez okres 36 miesięcy licząc od terminu instalacji Platformy, w zakresie
    a. Rozwiązywanie problemów i błędów pojawiających się w Platformie,
    b. Cyklicznie (raz na kwartał) przeglądy i weryfikacja poprawności działania Platformy oraz aktualizacja systemu i jego komponentów (w uzgodnieniu z Zamawiającym),
2. Prace rozwojowe, polegające m.in. na realizacji przez Wykonawcę zadań polegających m.in. na:
    - tworzeniu nowych playbooków,
    - integracji z nowymi systemami bezpieczeństwa,
    - konfiguracji nowych dashboardów,
    - budowanie nowych raportów.

   Prace te będą realizowane przez Wykonawcę na zlecenie Zamawiającego, w terminach i zakresie uzgodnionym z Zamawiającym, w wymiarze do 300 rbh (roboczogodzin).