

Załącznik nr 1 Opis potrzeb i wymagań Zamawiającego

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest kompleksowe świadczenie usług z zakresu bezpieczeństwa teleinformatycznego, obejmujących dostawę, wdrożenie, konfigurację, integrację oraz utrzymanie zaawansowanych systemów ochrony cyberbezpieczeństwa.

Zamówienie obejmuje:

1. **Security Operations Center (SOC)** – usługa zapewnienia całodobowego monitorowania, analizy oraz reakcji na incydenty bezpieczeństwa w środowisku teleinformatycznym Zamawiającego z wykorzystaniem systemu SIEM (Security Information and Event Management) Zamawiającego, opisanego w załączniku 1a.
2. **Security Orchestration, Automation and Response (SOAR)** – dostawę, wdrożenie i utrzymanie systemu automatyzacji i orkiestracji procesów bezpieczeństwa, wspierającego analizę i obsługę incydentów oraz integrację z istniejącymi narzędziami.
3. **System Decepcji (Deceptor)** – dostawę, wdrożenie i utrzymanie systemu wykrywania i analizy ataków z wykorzystaniem technologii honeypot, umożliwiającego detekcję aktywności niepożądanych wewnątrz sieci.
4. **System Uwierzytelniania, Autoryzacji i Kontroli Dostępu** – dostawę, wdrożenie i utrzymanie wysokowydajnego, skalowalnego systemu odpowiedzialnego za zapewnienie bezpiecznego dostępu użytkowników do zasobów teleinformatycznych.

Celem zamówienia jest podniesienie poziomu bezpieczeństwa Zamawiającego poprzez wdrożenie zintegrowanych rozwiązań technologicznych wspierających wykrywanie zagrożeń, automatyzację procesów, kontrolę dostępu oraz ochronę infrastruktury. Realizacja zamówienia ma zapewnić spójne i efektywne funkcjonowanie wszystkich elementów ekosystemu cyberbezpieczeństwa.

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie:

- 1) Instalacja i wdrożenie usługi SOC - nie później niż 60 dni od zawarcia umowy
- 2) usługę utrzymania wdrożonych systemów SOC przez okres 36 miesięcy od daty podpisania protokołu odbioru usług wskazanych w pkt. 1

Część 1 - Security Operations Center

1. Opis usługi

Usługa Security Operations Center (SOC) stanowi kompleksowe rozwiązanie w zakresie monitorowania, analizy oraz reagowania na incydenty bezpieczeństwa w infrastrukturze teleinformatycznej Zamawiającego. Celem usługi jest zapewnienie ciągłej (24/7/365) ochrony środowiska IT poprzez wczesne wykrywanie zagrożeń, minimalizację ryzyka wystąpienia incydentów oraz wsparcie w ich obsłudze i eliminacji skutków.

2. Instalacja i Wdrożenie

- 1) Wykonawca rozpocznie świadczenie usługi SOC nie później niż w ciągu 60 dni od daty zawarcia Umowy,
- 2) Jako rozpoczęcie świadczenia usługi rozumie się objęcie monitoringiem analityków Linii pierwszej w trybie pełnym systemu SIEM i podpisanie protokołu odbioru usługi,
- 3) Wykonawca przeprowadzi analizę przedwdrożeniową, określającą gotowość Zamawiającego do wdrożenia SOC oraz omówi z Zamawiającym wnioski wynikające z tej analizy,
- 4) Wykonawca, we współpracy z Zamawiającym, przeprowadzi szczegółową analizę
 - a) identyfikację kluczowych źródeł zdarzeń (m.in. serwery, stacje robocze, systemy operacyjne, urządzenia bezpieczeństwa, systemy uwierzytelniania, aplikacje krytyczne),
 - b) ustalenie sposobu ich normalizacji, parsowania i korelacji,
 - c) definicję reguł wykrywania incydentów bezpieczeństwa, alertów i wskaźników zagrożeń (IoC),
 - d) opracowanie modelu retencji i priorytetyzacji danych zgodnie z wymaganiami bezpieczeństwa oraz polityką Zamawiającego,
- 5) Wykonawca jest zobowiązany do zasilania swoich systemów dodatkowymi informacjami o zagrożeniach (Threat Intelligence) w ramach realizowanych działań operacyjnych SOC, w celu zwiększenia potencjału ochrony systemów oraz bieżącego wzbogacania danych o incydentach bezpieczeństwa, przede wszystkim o informacje dotyczące źródeł, charakteru, technik, klasyfikacji pod względem szkodliwości oraz wiarygodności
- 6) Wykonawca wraz z zamawiającym ustalą i wdrożą mechanizmy uwierzytelnienia oraz mechanizmy szyfrowania danych w czasie transmisji w sieci prywatnej i publicznej,

- 7) Wykonawca ustali z Zamawiającym klasyfikację incydentów, przedstawi propozycję minimum 100 scenariuszy reagowania na wykryte incydenty oraz dostarczy opis sposobu obsługi tych scenariuszy,
- 8) Jako podstawową kwalifikację incydentów przyjmuje się min.:
 - a) **Incydent krytyczny:** incydent wygenerowany na bazie logów pochodzących ze zdefiniowanych źródeł logów lub incydent wskazany przez Zamawiającego w zgłoszeniu jako uniemożliwiający prowadzenie podstawowej działalności operacyjnej,
 - b) **Incydent istotny:** incydent wygenerowany na bazie logów pochodzących ze zdefiniowanych źródeł logów lub incydent wskazany przez Zamawiającego jako utrudniający prowadzenie podstawowej działalności operacyjnej,
 - c) **Incydent niski:** incydent wygenerowany na bazie logów pochodzących ze zdefiniowanych źródeł logów lub incydent wskazany przez Zamawiającego w zgłoszeniu jako naruszający funkcjonującą u Zamawiającego politykę bezpieczeństwa.
- 9) Wykonawca będzie prowadził strojenie systemu SIEM w celu implementacji reguł oraz zmniejszenia ilości fałszywych alarmów przez cały okres świadczenia usługi.
- 10) Wykonawca przygotuje protokół zakończenia okresu wdrożenia, zawierający wykaz źródeł logów z systemu Zamawiającego oraz wykaz przygotowanych scenariuszy reagowania na wykryte incydenty,
- 11) Wykonawca gwarantuje składowanie logów otrzymanych od Zamawiającego oraz dostęp do nich w ramach zasobów Zamawiającego uwzględniając platformę przez czas nie krótszy niż 12 miesięcy w sposób umożliwiający ich wykorzystanie w celu dokonania analizy powłamaniowej lub przekazanie organom prowadzącym postępowanie związane z wystąpieniem incydentu.

3. Wymagania do platformy

- 1) Zamawiający informuje, że dysponuje systemem SIEM Fortinet opisanym w załączniku 1a. System ten musi być wykorzystany przy świadczeniu przedmiotowej usługi SOC.
- 2) Podstawowe parametry system SIEM:
 - a) Dwa procesory o minimalnych parametrach 2.4 GHz, 16 rdzeni/32 wątki, 24 MB cache.
 - b) 128GB pamięci operacyjnej minimum DDR4, ECC
 - c) Dwa dyski SSD klasy Read Intensive tworzące RAID0.
 - d) 8 Dysków SATA 6 Gb/s o pojemności co najmniej 8TB, w RAID6.

- e) Wydajność SIEM nie mniejsza niż 5 000 EPS (zdarzeń na sekundę odbieranych w trybie ciągłym.
- f) System operacyjny SIEM: FortiSIEM - firmy FORTINET
- 3) W przypadku, gdy zasoby obliczeniowe lub przestrzeń dyskowa wymagana przez oferowaną przez Wykonawcę usługę, przekraczają możliwości istniejącego środowiska Zamawiającego, Wykonawca zobowiązany jest dostarczyć wysokodostępne środowisko w postaci klastra obliczeniowego lub odpowiednio rozszerzyć obecne środowisko Zamawiającego.

1) Retencja Danych

- 1) Zamawiający wymaga, aby w ramach świadczonej usługi SOC i SOAR zapewniona była retencja:
 - a) szybkich logów na poziomie 30 dni;
 - b) historycznych logów na poziomie 365 dni.

5. Kopia zapasowa

Dostarczone rozwiązanie powinno być objęte mechanizmem tworzenia kopii zapasowych, umożliwiającym pełne odtworzenie środowiska po awarii lub incydencie, zgodnie z polityką bezpieczeństwa Zamawiającego.

6. Realizacja Usługi

- 1) Wykonawca będzie świadczył usługę w sposób spełniający wymagania zawarte w „Rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo”.
- 2) W ramach usługi Wykonawca zapewni monitorowanie bezpieczeństwa infrastruktury teleinformatycznej, systemów i działań użytkowników Zamawiającego w trybie 24/7/365,
- 3) Monitorowanie bezpieczeństwa infrastruktury Zamawiającego oznacza co najmniej:
 - a) analizę logów w czasie rzeczywistym,
 - b) reagowanie na incydenty – realizację uzgodnionych scenariuszy (w tym zamykanie zdarzeń typu False Positive),
 - c) raportowanie,
 - d) identyfikowanie i zarządzanie podatnościami,
 - e) aktualizację narzędzi bezpieczeństwa.
- 4) Zamawiający wymaga, aby usługa SOC świadczona przez Wykonawcę spełniała wskaźniki efektywności obsługi incydentu. Jako poprawne wartości przyjmuje się:

- a) Czas reakcji na incydent – 15 minut bez względu na typ incydentu (krytyczny, istotny, niski).
 - b) Czas reakcji rozumiany jest jako czas pomiędzy wykryciem incydentu bezpieczeństwa do momentu podjęcia działań po stronie zespołu SOC Wykonawcy,
 - c) Czas obsługi incydentu:
 - Krytycznego – 1h,
 - Istotnego – 4h,
 - Niskiego – 12h.
 - d) Czas obsługi rozumiany jest jako czas potrzebny do sklasyfikowania przeprowadzania analizy oraz podjęcia decyzji w kwestii ew. kontynuowania ścieżki eskalacji
Powyższe ma zastosowanie w przypadku 50 pierwszych incydentów danego dnia.
- 5) W celu poprawnego monitorowania bezpieczeństwa Wykonawca zapewni dostęp do Pierwszej, Drugiej i Trzeciej Linii Wsparcia.
- 6) Zespół analityków SOC powinien posiadać minimum 7 aktywnych certyfikatów, w tym certyfikaty potwierdzające kompetencje dla świadczonej usługi tj.:
- a) Certyfikat CompTIA Security+ lub równoważny;
 - b) Certyfikat Security Team – Blue Team Level 1 (BTL1) lub równoważny;
 - c) Certyfikat Red Team Professional lub równoważny;
 - d) Certyfikat ESET Managed Client Security Professional lub równoważny ;
 - e) Certyfikat CISSP – Certified Information Systems Security Professional lub równoważny
 - f) certyfikat CEH – Certified Ethical Hacker lub równoważny
 - g) przynajmniej jednego członka zespołu, który posiada ważne poświadczenia bezpieczeństwa, uprawniające do dostępu do informacji niejawnych o klauzuli Ściśle Tajne
- 7) Pierwsza Linia Wsparcia zapewnia:
- a) monitoring systemów i usług Zamawiającego w celu wykrywania zdarzeń mogących stanowić naruszenie bezpieczeństwa (incydentów) za pośrednictwem FortiSIEM oraz systemu SOAR,
 - b) bieżące odbieranie i rejestrowanie zgłoszeń telefonicznych oraz mailowych od Zamawiającego,
 - c) wstępną analizę i kwalifikację wykrytych zdarzeń, w tym potwierdzanie zasadności incydentu,

- d) reakcję na wykryte incydenty zgodnie z przygotowanymi scenariuszami działania (Runbookami/Playbookami) oraz warunkami określonymi w umowie SLA,
 - e) eskalowanie incydentów do Drugiej Linii Wsparcia zgodnie z ustalonymi procedurami i poziomem ich istotności,
 - f) prowadzenie komunikacji z Zamawiającym w zakresie statusu zgłoszeń i podejmowanych działań,
 - g) zamykanie zdarzeń typu False Positive po ich weryfikacji oraz dokumentowanie przebiegu obsługi incyduentu.
 - h) wstępną analizę podejrzanych plików pod kątem występowania złośliwego oprogramowania, z wykorzystaniem automatycznych narzędzi do analizy
- 8) Druga Linia Wsparcia zapewnia:
- a) obsługę incydentów bezpieczeństwa przekazanych przez Pierwszą Linie Wsparcia (L1), w szczególności incydentów o wysokim i krytycznym priorytecie, zgodnie z zaakceptowanymi scenariuszami bezpieczeństwa,
 - b) zarządzanie infrastrukturą systemu FortiSIEM,
 - c) zarządzanie systemem do orkiestracji zabezpieczeń, automatyzacji i reagowania typu SOAR,
 - d) administracja systemem służącym do zarządzania Honeypotami,
 - e) administracja systemem służącym do zarządzania tożsamością i dostępem,
 - f) monitorowanie dostępności, integralności i wydajności ww. systemów oraz reagowanie na zdarzenia wpływające na jego stabilność,
 - g) wdrażanie aktualizacji i poprawek bezpieczeństwa w elementach systemu FortiSIEM oraz powiązanych komponentach infrastruktury,
 - h) przygotowywanie rekomendacji zmian i usprawnień w konfiguracji lub politykach bezpieczeństwa w następstwie analizy obsługiwanych incydentów,
 - i) koordynację i komunikację techniczną pomiędzy zespołami Wykonawcy i Zamawiającego w ramach procesu obsługi incydentów,
 - j) strojenie systemu FortiSIEM, w tym optymalizację reguł korelacyjnych, filtrów, polityk powiadomień oraz progów alertowania,
 - k) opracowywanie i aktualizację scenariuszy działania (Runbooków/Playbooków) dla Pierwszej Linii Wsparcia,
 - l) szczegółową analizę podejrzanych plików, w przypadku, gdy automatyczna analiza oraz analiza pierwszej linii wsparcia dała

niejednoznaczne rezultaty, które nie pozwalają jednoznacznie stwierdzić, czy dany plik jest złośliwy,

9) Trzecia Linia Wsparcia zapewnia:

- a) analizę powłamaniową (post-incident analysis) mającą na celu identyfikację sposobu uzyskania dostępu, zasięgu kompromitacji, skutków incydentu oraz przygotowanie rekomendacji naprawczych i prewencyjnych,
 - b) prowadzenie informatyki śledczej (digital forensics), w tym zabezpieczanie i analizę danych dowodowych, rekonstrukcję zdarzeń oraz przygotowanie materiału analitycznego do celów raportowych lub prawnych,
 - c) cykliczne skanowanie i przekazanie spersonalizowanego raportu podatności systemów i usług zewnętrznych Zamawiającego, z uwzględnieniem nowych zagrożeń i luk bezpieczeństwa publikowanych przez producentów,
 - d) analizę typu reverse engineering, umożliwiającą dekompilację, zrozumienie i ocenę działania podejrzanych plików binarnych lub komponentów wykorzystywanych w incydentach bezpieczeństwa.
- W trakcie świadczenia usługi Zamawiający powinien mieć do dyspozycji maksymalnie 5000 roboczogodzin trzeciej linii wsparcia, przy ograniczeniu do 200 roboczogodzin miesięcznie:

- 10) Wykonawca zapewni wsparcie personelu Zamawiającego we wdrożeniach rekomendacji po wystąpieniach incydentów,
- 11) W przypadku niewykonywania działań określonych w rekomendacjach Wykonawca ma prawo do odstąpienia od realizacji usługi w zakresie źródła, którego dotyczy brak realizacji działań określonych w rekomendacjach.

7. Raportowanie

- 1) Wykonawca zapewni przekazywanie informacji zgodnie z punktem realizacji usługi o wykrytych incydentach do wyznaczonych pracowników Zamawiającego z użyciem uzgodnionych kanałów informacji: telefon, e-mail.
- 2) Wykonawca zapewni przekazywanie Zamawiającemu uzgodnionych co do treści i częstotliwości wykonywania, generowanych automatycznie cyklicznych raportów dotyczących wykrytych incydentów,
- 3) W raportach Wykonawca będzie przedstawiał ogólne rekomendacje z zakresu cyberbezpieczeństwa dla Zamawiającego, wynikające z

obsłużonych incydentów i mające na celu zapobieżenie powstaniu takich incydentów w przyszłości,

- 4) Wykonawca zapewni wsparcie Zamawiającemu w raportowaniu i przekazywaniu incydentów poważnych w rozumieniu ustawy o Krajowym Systemie cyberbezpieczeństwa do wskazanego CSIRT poziomu krajowego w ciągu 24 godzin od momentu ich wykrycia.

8. Wsparcie eksperckie

- 1) W ramach świadczonej Usługi Wykonawca ma za zadanie zapewnić (poprzez przedstawienie stosownych rekomendacji oraz zaleceń) optymalne działania systemów bezpieczeństwa, wykorzystywanych do świadczenia tej usługi. W przypadku identyfikacji nieprawidłowości Wykonawca w porozumieniu z Zamawiającym podejmie stosowne działania korygujące,
- 2) Wykonawca powinien aktywnie wspierać rozwój systemów bezpieczeństwa, które posiada Zamawiający.
- 3) Wykonawca zapewni cykliczne spotkania podsumowujące (raz na miesiąc) w celu wykonania transferu wiedzy oraz omówienia istotnych zdarzeń bezpieczeństwa, podatności czy problemów technicznych.

9. Dokumentacja

- 1) Wykonawca przygotuje i przedstawi projekt techniczny powstały na podstawie przeprowadzonej wcześniej wraz z Zamawiającym analizy przedwdrożeniowej,
- 2) Raport będzie zawierał co najmniej analizę potencjalnych źródeł logów (systemów i aplikacji), sposób ich normalizacji, parsowania i korelacji w SIEM w celu identyfikacji incydentów bezpieczeństwa, klasyfikację incydentów oraz listę scenariuszy,
- 3) Po zakończeniu wdrożenia Wykonawca przedstawi Dokumentację zawierającą co najmniej:
 - a) ostateczny kształt infrastruktury informatycznej wykorzystywanej do świadczenia usługi,
 - b) architekturę,
 - c) listę źródeł logów,
 - d) listę scenariuszy,
 - e) listę uzgodnionych sposobów komunikacji,
 - f) sposób powiadamiania o incydentach,
 - g) listę raportów przedstawianych Zamawiającemu podczas świadczenia Usługi.

Część 2 SOAR

Wymagania i potrzeby Zamawiającego w zakresie dostarczenia, wdrożenia, integracji i uruchomienia Systemu Security Orchestration Automation And Response (dalej SOAR) w środowisku teleinformatycznym Zamawiającego. Wykonawca musi przedłożyć oświadczenie producenta lub autoryzowanego partnera producenta, że posiada autoryzację producenta lub autoryzowanego partnera producenta w zakresie sprzedaży oferowanego rozwiązania

1. System musi zrealizować podstawowe cele stawiane przez Zamawiającego:

- 1) Udostępnienie jednego interfejsu i platformy pochodzących od tego samego producenta dla zarządzania, orkiestracji bezpieczeństwem informatycznym jak i automatyzacji działań i zadań
- 2) Zarządzanie incydentami bezpieczeństwa
- 3) Zautomatyzowanie powtarzalnych zadań w ramach zespołu SOC
- 4) Identyfikacja i rozróżnienie zagrożeń od fałszywych alarmów
- 5) Poprawa parametrów działania zespołu SOC
- 6) Ułatwienie zarządzania pracą zespołu SOC
- 7) Ustandaryzowanie procesów i procedur postępowania
- 8) Wprowadzenie parametrów oraz ich pomiaru, służących do raportowania wydajności i skuteczności obsługi zdarzeń bezpieczeństwa zarówno przez zespół jak i mechanizmy automatyzujące
- 9) Zdecydowaną redukcję powtarzalnych działań pracowników na rzecz automatycznych kroków i całych procesów

Szczegółowe wymagania opisano w tabeli poniżej.

ID	Opis
1.	System MUSI mieć możliwość instalacji w infrastrukturze Zamawiającego bez żadnego elementu wykonawczego, analitycznego lub innego znajdującego się poza infrastrukturą Zamawiającego.
2.	System MUSI mieć możliwość domyślnej instalacji w środowisku wirtualizacyjnym i MUSI wspierać co najmniej środowiska producentów VMWare oraz Red Hat KVM.
3.	System POWINIEN być dostarczony jako kompletny obraz do instalacji, zarówno systemu operacyjnego jak i oprogramowania. MUSI być dostępna opcja instalacji SOAR na własnym systemie operacyjnym Zamawiającego, co najmniej Red Hat.
4.	System SOAR MUSI mieć możliwość licencjonowania w ramach modelu subskrypcyjnego, gdzie licencje będą opłacane na określony czas działania rozwiązania.

	System SOAR MUSI też posiadać opcję licencjonowania w ramach modelu stałej licencji, nieograniczonej czasowo oraz wsparcia technicznego producenta działającego w ustalonym czasie.
5.	System MUSI posiadać licencjonowanie oparte o ilość użytkowników jednocześnie korzystających z systemu – sprawdzanie powinno być realizowane w oparciu o jednoczesne aktywne sesje zalogowanych użytkowników.
6.	System POWINIEN umożliwiać przypisywanie licencji na sesję dla kont imiennych, gdzie jedno konto zużywa jedną licencję oraz tworzenie kont wspólnych, które działają w ramach pozostałej puli dostępnych połączeń. Zmiana trybu licencji dla poszczególnych kont powinna być możliwa w dowolnym momencie.
7.	System SOAR NIE MOŻE licencjonować lub ograniczać innych parametrów systemu, jak ilość wykonywanych akcji, liczba podłączonych konektorów, rozmiar dysku, itp.
8.	System SOAR MUSI mieć możliwość szyfrowania danych zapisywanych na dysku lokalnym. Szyfrowanie takie musi być wspierane przez producenta oprogramowania, a sposób konfiguracji musi być opisany w publicznie dostępnej dokumentacji produktu.
9.	System MUSI mieć możliwość wyboru wielu języków interfejsu graficznego GUI. Musi istnieć możliwość zaimplementowania języka polskiego.
10.	System SOAR MUSI mieć możliwość instalacji oraz aktualizacji w trybie offline, tzn. bez dostępu systemu do Internetu. Wymaganie dotyczy również pracy z konektorami.
11.	Producent systemu MUSI dostarczać aktualizacje obejmujące zarówno system operacyjny jak i oprogramowanie SOAR.
12.	Aktualizacja konektorów NIE MOŻE powodować restartu systemu.
13.	Aktualizacja istniejących w systemie konektorów i obsługiwanych przez producenta MUSI być realizowana z poziomu GUI systemu, bez konieczności uruchamiania innego interfejsu. Aktualizacje MUSZĄ być widoczne w interfejsie systemu od momentu ich dostępności (dotyczy pracy w trybie online).
14.	Rozwiązanie 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.
15.	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.
16.	Wszystkie konektory MUSZĄ udostępniać swój 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.
17.	Tam gdzie to jest możliwe i zasadne konektory MUSZĄ wykorzystywać szyfrowane połączenia z systemem integrowanym, np. poprzez protokół SSL i weryfikację certyfikatu.
18.	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. SOAR MUSI posiadać możliwość importu konektorów z przygotowanego wcześniej archiwum.
19.	Producent MUSI dostarczyć zestaw bibliotek SDK (j. ang: Software Development Kit) dla łatwego tworzenia własnych konektorów.
20.	Oferowany system MUSI posiadać publicznie dostępne repozytorium dla integracji, konektorów, pakietów rozszerzeń np. GitHub. Repozytorium to MUSI być aktualizowane zarówno przez producenta jak i społeczność użytkowników.
21.	Oferowany system 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.
22.	Producent oferowanego systemu 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.

23.	Zamawiający wymaga, aby dla oferowanego systemu dostarczona była również wersja testowa. Wersja testowa POWINNA posiadać taką samą funkcjonalność i wersję jak produkcyjna. MUSI być możliwe uruchomienie więcej niż jednej instancji testowej.
24.	System SOAR MUSI umożliwiać importowanie części konfiguracji lub interfejsu z innego systemu, np. testowego.
25.	Interfejs graficzny MUSI udostępniać szatę kolorystyczną GUI co najmniej w jasnych barwach i ciemnych (darkmode).
26.	System SOAR 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.
27.	SOAR MUSI posiadać graficzny interfejs budowania i symulacji Playbook-ów.
28.	Edytor Playbook-ów MUSI udostępniać co najmniej następujące typy elementów wykonawczych: 1. Wykonanie zadania przez użytkownika technicznego SOAR (personel SOC/CSIRT) 2. Wykonanie zadania przez użytkownika biznesowego 3. Wykonanie automatycznego zadania w zintegrowanym z SOAR systemie bezpieczeństwa Zamawiającego 4. Wykonanie automatycznego zadania w elemencie infrastruktury teleinformatycznej Zamawiającego
29.	Projektowanie i wykonywanie Playbook-ów MUSI udostępniać możliwość złożonych ścieżek postępowania, w tym co najmniej: 1. Ścieżek równoległych 2. Ścieżek alternatywnych 3. Ścieżek warunkowych
30.	Playbook MUSI udostępniać możliwość budowania rozdzielnych ścieżek postępowania na każdym jego etapie w zależności od parametrów wejściowych dodanego elementu.
31.	Wykonywanie Playbook-ów MUSI udostępniać możliwość: 1. Rozwidlania na wiele ścieżek

	2. Zbieżności wielu ścieżek w jednym elemencie
32.	SOAR MUSI udostępniać możliwość budowania nowych Playbook-ów na bazie już istniejących poprzez kopiowanie i edycję.
33.	SOAR MUSI udostępniać możliwość wersjonowania Playbook-ów.
34.	System SOAR MUSI posiadać możliwość importu do Playbook-ów workflow z narzędzia BPMN. MUSI być obsługiwany format pliku źródłowego XML i JSON.
35.	SOAR MUSI udostępniać możliwość tworzenia Playbook-ów zagnieżdżonych tzn. korzystających z już istniejących, gdzie istniejący Playbook jest częścią utworzonego nowego playbook-a.
36.	SOAR MUSI posiadać mechanizmy wyboru ścieżki/ścieżek w Playbook-ach na podstawie kontekstu danych/parametrów.
37.	SOAR MUSI się integrować z zewnętrznymi systemami CTI (Cyber Threat Intelligence).
38.	System 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.
39.	Producent SOAR MUSI dostarczać własną bazę CTI (Cyber Threat Intelligence) możliwą do uruchomienia w systemie.
40.	System MUSI posiadać interfejsy pozwalające na integrację z rozwiązaniami CyberThreatIntelligence (STIX, TAXII).
41.	Integracja z CTI MUSI umożliwiać pobieranie przez System SOAR 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.).
42.	SOAR MUSI posiadać możliwość wprowadzania informacji o Incydentach różnymi interfejsami w tym co najmniej: <ul style="list-style-type: none"> 1. Poprzez Operatora manualnie 2. Poprzez integracje z systemem ServiceDesk (zdarzenie zakwalifikowane jako Incydent cyberbezpieczeństwa) 3. Poprzez integracje z systemami bezpieczeństwa

	<p>4. Przez SIEM</p> <p>5. Porzez pocztę elektroniczną – dedykowane konto dla powiadomień</p>
43.	<p>System SOAR MUSI posiadać możliwość definiowania w sposób ustrukturyzowany danych o Incydencie w postaci artefaktów. Co najmniej MUSZĄ być wspierane domyślnie następujące rodzaje:</p> <ol style="list-style-type: none"> 1. pliki 2. skróty danych w postaci SHA1, SHA256, MD5 3. adresy IP 4. adresy URL 5. nazwy DNS 6. Hostname 7. Port 8. Rejestr 9. użytkownik 10. proces 11. adres email
44.	System SOAR MUSI mieć możliwość dowolnego definiowania nowych typów artefaktów.
45.	SOAR POWINIEN mieć możliwość tworzenia skryptów w co najmniej języku programowania PYTHON.
46.	SOAR MUSI mieć domyślnie zdefiniowane co najmniej 5 stopni istotności Incydentów. Ilość stopni jak i ich nazwy POWINNY udostępniać możliwość definiowania.
47.	SOAR MUSI mieć możliwość TAG-owania zdarzeń przekazywanych do SOAR, alertów, zadań i incydentów.
48.	<p>SOAR MUSI mieć możliwość definiowania SLA na poziomie:</p> <ol style="list-style-type: none"> 1. Alarmów 2. Incydentów
49.	SOAR MUSI mieć możliwość definiowania ról w zakresie rozwiązywania, zarządzania i raportowania incydentów bezpieczeństwa.
50.	<p>SOAR MUSI mieć możliwość definiowania co najmniej pięciu rodzajów ról ze względu na uprawnienia:</p> <ol style="list-style-type: none"> 1. Menadżer Incydentów 2. Pracownik I linii SOC 3. Pracownik II linii SOC 4. Pracownik III linii SOC 5. Użytkownik biznesowy

51.	SOAR MUSI posiadać możliwość integracji z posiadanym przez Zamawiającego systemem SIEM (FortiSIEM) w zakresie: 1. przekazywania informacji o Incydentach, mapowania poszczególnych pól 2. Wzbogacanie informacji o incydentach bezpośrednio z dodatkowych akcji API wykonywanych na SIEM poprzez SOAR 3. Wykonywania procedur SOAR bezpośrednio z poziomu SIEM 4. Wykonywania akcji SOAR bezpośrednio z poziomu SIEM Integracja musi być realizowana przez obu dostawców domyślnie i udokumentowana w momencie składania oferty.
52.	SOAR MUSI mieć możliwość załączania plików.
53.	SOAR MUSI mieć możliwość zamieszczania komentarzy w zadaniach.
54.	SOAR MUSI mieć możliwość cyklicznego uruchamiania Playbook-ów według ustalonego harmonogramu.
55.	SOAR MUSI umożliwiać przechowywanie danych o Incydentach z pełną informacją o operacjach wykonanych w systemie w zadanym okresie czasu..
a.	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.
56.	SOAR Moduł War Room 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
57.	SOAR MUSI mieć możliwość personalizowania widoków w interfejsach dla użytkowników.
58.	SOAR MUSI posiadać mechanizmy integracji z systemami bezpieczeństwa oraz infrastrukturą teleinformatyczną w zakresie: Wymienić listę podstawowych integracji
59.	SOAR POWINIEN posiadać mechanizmy integracji z systemami bezpieczeństwa oraz infrastrukturą teleinformatyczną w zakresie: Wymienić listę opcjonalnych integracji

60.	SOAR MUSI mieć możliwość definiowania cyklicznego generowania raportów..
61.	SOAR MUSI posiadać mechanizmy logowania zdarzeń i operacji wykonywanych przez użytkownika.
62.	SOAR MUSI posiadać mechanizmy uwierzytelniania w oparciu o Active Directory i protokół SAML.
63.	Zarządzanie uprawnieniami MUSI być oparte o role.
64.	SOAR MUSI posiadać mechanizmy uwierzytelnia wieloskładnikowego.
65.	SOAR MUSI posiadać mechanizmy integracji z systemami PAM.
66.	SOAR MUSI posiadać interfejs użytkownika udostępniany poprzez https.
67.	SOAR MUSI mieć możliwość automatycznego powiązania i grupowania podobnych incydentów (np. ten sam docelowy adres IP, usługa itp.)
68.	System SOAR 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.	Rozwiązanie 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: <ol style="list-style-type: none"> 1. Wiele-do-wiele 2. Wiele-do-jednego
71.	Rozwiązanie 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.	System 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.	<p>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:</p> <ol style="list-style-type: none"> 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.	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.
78.	Rozwiązanie MUSI być zintegrowane z MITRE ATTACK, przez którą to możliwe będzie wzbogacenie analizy incydentów o informacje takie jak: taktyki, analiza zagrożenia i sugestie dotyczące środków zaradczych.
79.	<p>System MUSI umożliwiać skonfigurowanie obowiązkowego uzupełnienia notatek przez operatora przed zamknięciem dochodzenia, dla incydentu obejmującego co najmniej sekcje:</p> <ol style="list-style-type: none"> 1. informacja podsumowująca 2. następne kroki 3. opis sposobu rozwiązania problemu <p>Każde pole MUSI mieć możliwość wyboru konfiguracji: nieobowiązkowe, obowiązkowe, warunkowo obowiązkowe.</p>

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.	Rozwiązanie MUSI mieć konfigurowalną funkcję zarządzania kolejkami obsługującą automatyczne przypisywanie alertów/incydentów/zadań do różnych grup obsługujących.
82.	Rozwiązanie 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.	Rozwiązanie 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: <ol style="list-style-type: none"> 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 zadany wzorcem (pattern)

	<p>9. nie jest zgodny z zadany wzorcem (pattern)</p> <p>Warunki MUSZĄ obsługiwać sumę logiczną (dowolny warunek spełniony) oraz iloczyn logiczny (wszystkie warunki muszą być spełnione).</p>
87.	<p>Playbook-i MUSZĄ obsługiwać następujące sposoby uruchomienia:</p> <ol style="list-style-type: none"> 1. analityk może ręcznie uruchomić w GUI systemowym 2. automatycznie przy zmianie rekordu (Alert, wskaźnik, incydent... itd.): utworzony/zmieniony/usunięty 3. przez API: gdy SOAR otrzymał żądanie API z określonymi parametrami to uruchamia określonego Playbook-a 4. referencja: playbook ma możliwość wykonania innego playbook-a z zadanymi parametrami
88.	<p>System 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.</p>
89.	<p>Graficzny edytor Playbook-ów MUSI mieć możliwość cofania kroków edycji jak i ich ponawiania. Przykładowo możliwe jest przywrócenie wcześniej usuniętej operacji.</p>
90.	<p>Rozwiązanie 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.</p>
91.	<p>Administratorzy muszą mieć możliwość indywidualnego eksportowania i importowania Playbook-ów, w tym dowolnie wybranej wersji (podobnie jak SVN / GIT).</p>
92.	<p>Rozwiązanie MUSI obsługiwać tworzenie, modyfikowanie i usuwanie zmiennych globalnych dostępnych dla wszystkich Playbook-ów. Zmienne globalne muszą być edytowalne za pomocą Playbook-ów lub GUI.</p>
93.	<p>System MUSI dostarczyć wizualną historię wykonania Playbook-ów, która identyfikuje dane wyjściowe, wejściowe i konfigurację każdego kroku.</p>

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.																						
95.	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.																						
96.	Kontrola praw dostępu (RBAC) MUSI obejmować Playbook-i w zakresie zapisu i uruchamiania.																						
97.	Rozwiązanie 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.																						
98.	<p>Kroki warunkowe w wykonywaniu Playbook-ów muszą być wystarczająco elastyczne, aby móc stosować złożone warunki. Wymagane możliwości budowania warunków:</p> <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 wyrażenie 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> </table>	równy	porównuje dwa obiekty i wykonuje operację, gdy równe	nierówna się	porównuje dwa obiekty i wykonuje operację, gdy nie równe	większy niż	prawda, jeśli lewa strona jest większa niż prawa strona	większy niż lub równy	prawda, jeśli lewa strona jest większa lub równa prawej stronie	mniejsze niż	prawda, jeśli lewa strona jest mniejsza niż prawa strona	mniejsze lub równe	prawda, jeśli lewa strona jest mniejsza lub równa prawej stronie	i	zwróć wartość „prawda”, jeśli lewe i prawe wyrażenie są prawdziwe	lub	zwróć wartość „prawda”, jeśli lewe lub prawe wyrażenie jest prawdziwe	nie	negacja	dodawanie	dodaje do siebie dwa obiekty	odejmowanie	odejmij drugą liczbę od pierwszej
równy	porównuje dwa obiekty i wykonuje operację, gdy równe																						
nierówna się	porównuje dwa obiekty i wykonuje operację, gdy nie równe																						
większy niż	prawda, jeśli lewa strona jest większa niż prawa strona																						
większy niż lub równy	prawda, jeśli lewa strona jest większa lub równa prawej stronie																						
mniejsze niż	prawda, jeśli lewa strona jest mniejsza niż prawa strona																						
mniejsze lub równe	prawda, jeśli lewa strona jest mniejsza lub równa prawej stronie																						
i	zwróć wartość „prawda”, jeśli lewe i prawe wyrażenie są prawdziwe																						
lub	zwróć wartość „prawda”, jeśli lewe lub prawe wyrażenie jest prawdziwe																						
nie	negacja																						
dodawanie	dodaje do siebie dwa obiekty																						
odejmowanie	odejmij drugą liczbę od pierwszej																						

	dzielenie	dzielenie dwóch liczb
	modulo	obliczanie reszty z dzielenia liczby całkowitej
	mnożenie	mnożenie dwóch wartości
	potęga	podnieś lewy operand do potęgi prawego operandu
<p>Warunki takie jak:</p> $(zmienna_X + zmienna_Y)/2 > 3$ $((zmienna_X + zmienna_Y)/2 > zmienna_Z) \text{ OR } (zmienna_A / zmienna_B) < 2$ <p>muszą być możliwe bez użycia języka programowania .Etap podejmowania decyzji MUSI mieć opcję ustawienia domyślnego następnego kroku, jeśli wszystkie warunki zawiodą.</p>		
99.	Operatorzy muszą mieć możliwość zastosowania języka programowania, co najmniej Python bezpośrednio w Playbook-ach. Administrator SOAR MUSI być w stanie ograniczyć dostęp i możliwość wykorzystania bibliotek języka python (z dokładnością do pojedynczych bibliotek).	
100.	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.	
101.	Zarządzanie Playbook-ami MUSI umożliwiać analitykom zbiorczą ich edycję z możliwością wykonywania poniższych funkcji: <ol style="list-style-type: none">1. Zmiana statusu (Playbook aktywny lub nieaktywowany)2. Klonowanie wybranych Playbook-ów3. Przenoszenie wybranych Playbook-ów do innej grupy4. Zmiana poziomu logowania dla wybranych Playbook-ów5. Eksportowanie wybranych Playbook-ów	
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: <ol style="list-style-type: none">1. sklonuj krok	

	<p>2. kopiuj i wklej krok lub grupę kroków do tego samego Playbook-a lub innego</p> <p>3. wyrównaj wizualnie kroki na diagramie do układu pionowego lub poziomego</p> <p>- wybierz krok lub grupę kroków i usuń je</p>
104.	<p>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.</p>
105.	<p>System 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..</p>
106.	<p>System MUSI zapewnić pulpit (dashboard) z informacją o kondycji konektorów, który wskazuje, czy wszystkie integracje z systemami zewnętrznymi działają prawidłowo.</p>
107.	<p>Akcje konektorów muszą podlegać prawom dostępu RBAC tak aby tylko zdefiniowane role mogły używać zdefiniowanych akcji z dokładnością do pojedynczej akcji.</p>
108.	<p>System MUSI umożliwiać analitykowi uruchamianie dowolnej akcji konektora do której ma prawo, za pośrednictwem interfejsu GUI bez użycia Playbook-a.</p>
109.	<p>Musi istnieć możliwość zbiorczego importu i eksportu wskaźników IOC bezpośrednio z GUI.</p>
110.	<p>Rozwiązanie MUSI być na tyle elastyczne, aby umożliwić generowanie reputacji wskaźników na podstawie danych z różnych źródeł Threat Intelligence jednocześnie.</p>
111.	<p>Rozwiązanie MUSI umożliwiać tworzenie kopii zapasowych i przywracanie zarówno konfiguracji systemu, jak i zebranych danych.</p>
112.	<p>Rozwiązanie 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.</p>

113.	Architektura systemu MUSI pozwalać na skalowanie rozwiązania jak i tworzenie wysokiej dostępności. Musi istnieć możliwość klastrowania wielu węzłów (minimum 3) w konfiguracji Aktywny/Aktywny.
114.	Rozwiązanie MUSI oferować skalowalną geograficznie, rozproszoną architekturę z możliwością separacji części zasobów dla podległych jednostek lub innych użytkowników (model pracy MSSP).
115.	Rozwiązanie MUSI umożliwiać uruchamianie Playbook-ów i kolekcję danych w zdalnych segmentach sieci za pośrednictwem agenta SOAR wdrożonego w segmencie sieci zdalnej. Agenty muszą obsługiwać automatyczne aktualizacje.
116.	System MUSI umożliwiać korzystanie zarówno z wewnętrznej, jak i zewnętrznej bazy danych.
117.	Rozwiązanie MUSI oferować aplikację mobilną co najmniej dla systemu Android do zdalnego zarządzania i monitorowania w ramach SOAR.
118.	System 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.	System MUSI mieć możliwość przesyłania zdarzeń audytu i aplikacji do serwera zewnętrznego lub rozwiązania SIEM. Następujące protokoły muszą być obsługiwane z konfigurowalnym poziomem dziennika: <ol style="list-style-type: none"> 1. UDP 2. TCP, TCP/TLS 3. RELP, RELP/TLS
120.	System 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.	System 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.	1. SOAR 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

	<p>2. grupa równoważna (sibling) – ma dostęp do danych grup w ramach ustawionego połączenia</p> <p>3. grupa podrzędna (child) – brak możliwości dostępu do danych z nadrzędnych grup</p>
123.	System powinien zapewniać wiele konfigurowalnych pulpitów nawigacyjnych (dashboard), które działają zgodnie z prawami dostępu RBAC.
124.	System powinien zapewniać mechanizm wyróżniania alertów, które zbliżają się do naruszeń SLA.
125.	Pulpit nawigacyjny powinien móc wyświetlać informacje specyficzne dla analityka, takie jak alerty i zadania przypisane do niego.
126.	SOAR powinien obliczać szacowany zwrot z inwestycji i wyświetlenie go na pulpicie (dashboard).
127.	Powinno być możliwe importowanie i eksportowanie szablonów pulpitu nawigacyjnego.
128.	System powinien posiadać skonfigurowane pulpity nawigacyjne dedykowane dla ról, takich jak: analityk linii 1, analityk linii 2, menedżer SOC.
129.	SOAR 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.
130.	Rozwiązanie MUSI mieć dedykowany pulpit nawigacyjny do monitorowania stanu/dostępności każdej integracji, a także kondycji systemu SOAR.
131.	Rozwiązanie MUSI obsługiwać dostosowanie znaków graficznych (branding) interfejsu użytkownika dla różnych domen MSSP.
132.	Rozwiązanie MUSI zapewniać framework dla przygotowania własnego pulpitu nawigacyjnego zgodny z HTML/JSON/JS, aby umożliwić tworzenie niestandardowych widżetów pulpitu nawigacyjnego i importowanie ich do rozwiązania SOAR.
133.	System MUSI zapewniać konfigurowany moduł raportowania w GUI.
134.	Raporty MUSZĄ mieć możliwość zaplanowania uruchamiania w czasie zdefiniowanym przez użytkownika.
135.	Raporty MUSZĄ być generowane w co najmniej formatach CSV i PDF.
136.	Wygenerowane raporty MUSZĄ mieć opcję wysłania pocztą elektroniczną.

137.	MUSI być możliwe uruchamianie raportów z poziomu playbook.
138.	Dostęp do raportów MUSI być ograniczany prawami dostępu RBAC.
139.	System MUSI posiadać logi audytu, które dostarczą informacji o aktywności modułu raportowego, włączając akcję pobrania raportu.
140.	MUSI istnieć możliwość dołączania do raportu grafik i wykresów.
141.	<p>System MUSI posiadać moduł zarządzania zmianą operatorów, w szczególności MUSZĄ być obsługiwane funkcje:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a) filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne) b) poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione) 5. musi być możliwe przypisanie rekordu: <ol style="list-style-type: none"> a) nie przypisany b) przypisany kierownikowi zmiany c) wg. metody round robin w ramach członków zmiany
142.	<p>System 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:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a) utworzenie lub aktualizacja rekordu

	<p>b) filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne)</p> <p>c) poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione)</p> <p>4. musi być możliwe ustawienie priorytetu rekordu w ramach kolei</p> <p>5. musi być możliwe przypisanie rekordu:</p> <p>a) nie przypisany</p> <p>b) przypisany kierownikowi grupy</p> <p>c) wg. metody roundrobin w ramach członków grupy</p>
--	---

2. Wsparcie integracji z zewnętrznymi systemami

Wymaga się, aby oferowany system miał co najmniej 640 gotowych integracji.

3. Wymiarowanie systemu

Dostarczony system SOAR musi spełniać następujące wymagania licencyjne:

3.1 Licencja musi być dostarczona w formie licencji na wieczyste użytkowanie (ang: perpetual) z gwarancją i wsparciem producenta na okres 3 lat od daty końcowego odbioru

3.2 Licencja nie może w żaden sposób ograniczać ilości wykonywanych akcji przez system, ilości integracji, rozmiaru dysku, skonfigurowanych kont użytkowników.

3.3 System musi mieć umożliwiać jednoczesną pracę co najmniej pięciu administratorów lub operatorów.

Część 3 Deceptor

Dostarczenie rozwiązania do wykrywania i analizy ataków za pomocą technologii „honeypot”.

1. Wymagania ogólne

- 1) Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej.
- 2) System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji.
- 3) System powinien umożliwiać lokalne logowanie i raportowanie oraz współpracować z systemem centralnego logowania i raportowania.
- 4) Musi istnieć możliwość integracji systemu z rozwiązaniami zabezpieczeń klasy NGFW (Next Generation Firewall) oraz rozwiązaniami EDR (Endpoint Detection and Response).
- 5) Dla zapewnienia szybkiego wsparcia technicznego ze strony Wykonawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcie i aktualizacje oprogramowania.
- 6) Wykonawca musi przedłożyć oświadczenie producenta lub autoryzowanego partnera producenta, że posiada autoryzację producenta lub autoryzowanego partnera producenta w zakresie sprzedaży oferowanego rozwiązania

2. Parametry fizyczne systemu

- 1) Wymagania dla głównej maszyny:
System musi być wyposażony w co najmniej:
 - a) 4 interfejsy 1GE RJ45
 - b) 4 interfejsy 1GE SFP
 - c) 48 GB pamięci RAM
 - d) 2 TB przestrzeń dyskowej
 - e) Montowany w szafie technicznej 19 cali o standardowej wysokości 1U
 - f) Zużycie energii do 260W
 - g) Redundantne zasilacze
- 2) Wymagania dla zdalnych maszyn:
System musi być wyposażony w co najmniej:
 - a) 10 interfejsów 1GE RJ45
 - b) 4 GB pamięci RAM
 - c) Obudowa typu desktop
 - d) Chłodzenie pasywne bez wentylatorów

e) Zużycie energii do 20W

3. Funkcje szczegółowe systemu ochrony

- 1) System musi umożliwiać identyfikację cyberprzestępców lub pracowników mających złe zamiary (insider) znajdujących się wewnątrz sieci Zamawiającego. Identyfikacja musi bazować na raportowaniu skanowania, logowania, „dotykania” wystawionych plików na udziałach sieciowych, wysyłania komend we wspieranych protokołach, wchodzenia w interakcję z wystawionymi systemami pułapkami oraz przynętami/usługami.
- 2) System musi śledzić działania atakujących na pułapkach w czasie rzeczywistym i raportować adres IP, użyte dane uwierzytelniające, uruchomione i zatrzymane procesy, wykonane polecenia, np. w systemie Linux wraz z akcjami i technikami Industrial Control Systems, którymi posługuje się atakujący w interakcji z pułapkami i przynętami/usługami.
- 3) Powyższe incydenty generowane w czasie rzeczywistym muszą być korelowane w grupy oraz kampanie z uwzględnieniem ważności danego incydentu w zależności od akcji, które wykonał atakujący.
- 4) System musi skanować antywirusowo pliki dostarczane do pułapek, skanować systemem IDS ruch generowany od atakującego do pułapek (włącznie z sygnaturami IDS dla systemów Industrial Control Systems), skanować silnikiem webowym ruch generowany z systemów pułapek do Internetu.
- 5) Wsparcie dla systemów pułapek i przynęt:
 - a) emulujących pełny system operacyjny, w tym minimalnie:
 - (1) Windows 10
 - (2) Windows 11
 - (3) Windows 2016
 - (4) Windows 2019
 - (5) Windows 2022
 - (6) Ubuntu
 - (7) CentOS
 - (8) Red Hat Enterprise Linux
 - b) emulujących następujące systemy i przynęty/usługi wewnątrz nich, minimalnie:
 - a) CentOS, usługi SSH, SAMBA, HTTP, HTTPS, GIT, TCPListener. ICMP, FTP
 - b) Windows, usługi RDP, SMB, TCPListener, NBNSSpoofSpotter, HTTP/HTTPS, MSSQL, ICMP, FTP, SMTP

- c) MacOS
- d) Firewall
- e) usługa SSLVPN. W ramach tej usługi system musi mieć możliwość weryfikacji użytych parametrów logowania (login) w centralnym magazynie kont, np. Active Directory. Dzięki temu możliwe będzie odfiltrowanie szumu od prób logowania na realne konta danego środowiska.
- f) System CRM, usługa webowy ERP
- g) Webmin (interfejs html do zarządzania systemami linux)
- h) Systemy typu SCADA:
 - (a) Liebert Spruce UPS, usługi TFTP, SNMP, HTTP
 - (b) Schneider Power Meter - PM5560, usługi SNMP, BACNET, HTTP, DNP3, ENIP
 - (c) MOXA NPORT 5110, usługi SNMP, Telnet, HTTP, MOXA
 - (d) Rockwell 1769-L35E Ethernet Port, usługi SNMP, ENIP, HTTP
 - (e) GE PLC 90, usługi SNMP, HTTP, SRTP
 - (f) Kamstrup 382, usługi KAMSTRUP
 - (g) Siemens S7-200 PLC, usługi HTTP, TFTP, SNMP, MODBUS, S7COMM
 - (h) VAV-DD BACnet controller, usługi SNMP, BACNET
 - (i) Niagra4 Station, usługi SNMP, HTTP, BACNET
 - (j) Schneider EcoStruxure BMS server, usługi SNMP, HTTP, TRICONEX, BACNET
 - (k) Schneider Electric Modicon M241
 - (l) Rockwell PLC, usługi HTTP, TFTP, SNMP, ENIP
 - (m) NiagaraAX Station, usługi SNMP, HTTP, BACNET
 - (n) Rockwell 1769-L16ER/B LOGIX5316ER, usługi SNMP, ENIP, HTTP
 - (o) Guardian-AST, usługi Guardian-AST
 - (p) Schneider SCADAPack 333E, usługi SNMP, DNP3, Telnet
 - (q) Siemens S7-300 PLC, usługi TFTP, SNMP, IEC104
 - (r) IPMI Device, usługi HTTP, FTP, SNMP, IPMI
 - (s) Siemens S7-1500 PLC, usługi HTTP, TFTP, SNMP, IEC104, PROFINET
 - (t) Phoenix contact AXC 1050, usługi HTTP, SNMP, PROFINET, FTP
 - (u) PowerLogic ION7650, usługi SNMP, MODBUS, DNP3, HTTP
 - (v) Ascent Compass MNG, usługi HTTP, FTP, SNMP, IPMI, BACNET
 - (w) Modicon M241 oraz M580, usługi TFTP, SNMP, MODBUS, ENIP, HTTP

- (x) Emerson iPro by Dixell, usługi SNMP, MODBUS, HTTP
- (y) C-More HMI (ekrany dotykowe), usługi SNMP, HTTP, FTP, HTTPS
- (z) Lantronix XPORT, usługi SNMP, HTTP, Lantronix Discovery Protocol
- i) Ubuntu:
 - (a) Elastic Search, usługa Elastic Search
 - (b) Linux, usługi SSH, SAMBA, TCPListener, HTTP, HTTPS, GIT, ICMP, FTP, RADIUS, SMTP
 - (c) ESXi Decoy, usługi SSH, HTTP, HTTPS
 - (d) Tomcat, usługi HTTP, HTTPS
 - (e) MariaDB, usługa MariaDB
 - (f) ESXi, usługi SSH, HTTP, HTTPS
 - (g) ScadaBR, usługa ScadaBR
 - (h) Nginx, usługi HTTP, HTTPS
 - (i) Webmin, usługi HTTP, HTTPS
 - (j) Citrix ADC, Application Delivery Management, Gateway, Endpoint Management, Receiver, usługi HTTP, HTTPS
 - (k) TrueNAS, usługi SSH, SAMBA, HTTP, HTTPS, SNMP
- j) POS, usługa POS-WEB
- k) IOT:
 - (a) drukarka Lexmark, usługi SNMP, Jetdirect, Printer-WEB
 - (b) drukarka HP, usługi SNMP, Jetdirect, Printer-WEB
 - (c) router Cisco, usługi Telnet, HTTP, SNMP, CDP
 - (d) drukarka Brother MFC, usługi SNMP, Jetdirect, Printer-WEB
 - (e) router TP-LINK, usługi TP-Link WEB, CWMP
 - (f) kamera IP, usługi IP Camera-WEB, UPnP, SNMP, RTSP
 - (g) przełącznik HP, usługi SNMP, Telnet, CDP, HTTP
 - (h) router MikroTik, usługi SNMP, Telnet, CDP, HTTP
 - (i) router Netgear, usługi UPnP, SNMP, HTTP
- l) Medyczne:
 - (a) PACS, usługi Infusion Pump (Telnet), Infusion Pump (FTP)
 - (b) SPACECOM, usługi HTTP, HTTPS, FTP, CAN bus Protocol, SSH
 - (c) INFUSOMAT, usługi HTTP, HTTPS, FTP, CAN bus Protocol, B.BRAUN
- m) Telekomunikacyjne:
 - (a) Pułapka 4G/5G poprzez użycie oprogramowania NextEPC zawierającego Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW), Home

Subscriber Server (HSS) oraz Policy and Charging Rules Functions (PCRF)

(b) Obsługa protokołów SCTP, GTP-C oraz GTP-U

n) SAP, usługi SAP ROUTER, SAP DISPATCHER, SAP WEB

o) VOIP, usługi MQTT WEB, CoAP, SIP, XMPP WEB

p) SWIFT Lite 2, SWIFT VPN

c) dedykowany system dostarczany przez producenta zawierający przynętę/usługę podatną na atak/ataki, które mają duże konsekwencje dla całej branży cyberbezpieczeństwa i wpływają na wiele organizacji na świecie. Emulacja podatności musi być możliwa również w środowisku izolowanym. Wymaga się, aby system emulował minimalnie podatności dla:

a) Spring4Shell,

b) Log4j2,

c) CenOS Web Panel,

d) Cacti,

e) IBM Aspera Faspex,

f) ABB TotalFlow,

g) MOVEit,

h) Ivanti,

i) PAN-OS GlobalProtect Command Injection,

j) Palo Alto Networks PAN-OS Management Interface,

k) Apache Struts 2 Remote Code Execution

d) umożliwiających umieszczenie pułapek w środowisku chmurowym – minimalnie AWS, Azure, GCP.

6) Powyższe przynęty/usługi muszą być interaktywne w relacji z atakującym, w tym minimalnie:

a) przynęta/usługa udająca kamery, musi umożliwiać wgranie własnych nagrań w formacie mp4, które mogą zostać następnie zapętlone

b) przynęta/usługa udająca drukarki Lexmark, HP, Brother musi udostępniać webowe GUI, z którym atakujący może wejść w interakcje

c) przynęta/usługa routera Cisco musi umożliwiać wgranie własnej konfiguracji oraz umożliwiać zalogowanie się do systemu, włącznie z możliwością włączenia CDP

d) przynęta/usługa SAP musi umożliwiać połączenia do GUI po http/https z wykorzystaniem SAP Fiori Lanuchpad lub WebGUI

e) przynęty/usługi SNMP muszą umożliwiać konfigurację własnego Community

f) przynęty/usługi SCADA muszą umożliwiać łapanie ataków przez odpowiadające im usługi, czyli IEC104, S7COMM, MODBUS, telnet

- g) przynęta/usługa ESXi musi umożliwiać zalogowanie się do systemu poprzez SSH oraz WebGUI
- 7) Przynęta/usługa TCPLListener dla systemów Windows i Linux musi umożliwiać konfigurację dowolnego portu, na którym przynęta/usługa nasłuchuje i raportować w GUI/logu, że połączenie na taki port nastąpiło.
- 8) Systemy operacyjne/pułapki muszą wspierać wykrywanie ataków w warstwie 2, wykrywając minimalnie MITM, ICMP Swiping i Responder.
- 9) Systemy operacyjne/pułapki Windows muszą wspierać podanie konkretnych par użytkownik/hasło, wspierając podanie minimalnie 5 taki par. W wypadku integracji z dostosowanym systemem Windows podłączonym do Active Directory mogą zostać wykorzystane dowolne pary użytkownik/hasło.
- 10) System musi wspierać instalację dedykowanego oprogramowania na realnych stacjach końcowych, które to programowanie będzie mapowało lokalnie dysk na jedną z wystawionych pułapek. Oprogramowanie musi wspierać instalację minimalnie z wykorzystaniem Active Directory GPO.
- 11) Dedykowane oprogramowanie musi wspierać zapisanie w rzeczywistej stacji końcowej w Windows Vault nazwy konkretnego użytkownika i hasła.
- 12) Dedykowane oprogramowania musi wspierać generowanie oraz dystrybucję nieprawdziwych kluczy dostępowych od usług Amazon Web Services.
- 13) System musi umożliwiać utworzenie fałszywego zasobu plikowego z własnoręcznie przygotowanych plików.
- 14) System musi umożliwiać utworzenie fałszywego zasobu plikowego bazując na realnym systemie plików. Musi być możliwość odwzorowania wszystkich lub wskazanych katalogów. Musi być możliwość ustawienia częstotliwości z jaką taki klon będzie odświeżany.
- 15) System musi umożliwiać konfigurację resetu całej pułapki w razie wykrycia intruza, reset następuję po wskazania określonego czasu od wykrycia zdarzenia.
- 16) System musi wspierać możliwość instalacji specyficznego oprogramowania do zarządzania SCADA wewnątrz systemów Windows (np. RAPID SCADA).
- 17) System musi reagować na incydenty, wykonać kwarantannę, poprzez integrację z zewnętrznymi systemami.
- 18) Kwarantanna minimalnie musi być możliwa poprzez integrację z zewnętrznymi systemami bezpieczeństwa takimi jak:
- a) firewall Checkpoint
 - b) firewall FortiGate
 - c) firewall PaloAlto
 - d) system Cisco ISE

- e) system FortiNAC
 - f) system CrowdStrike
 - g) system FortiEDR
 - h) Aruba ClearPass
 - i) system Microsoft ATP
 - j) Sentinel One EDR
- 19) Kwarantanna musi być możliwa poprzez integrację z zewnętrznymi systemami bezpieczeństwa z wykorzystaniem REST API. W zakresie integracji musi być możliwe skonfigurowanie:
- a) osobna konfiguracja dla akcji blokuj oraz odblokuj
 - b) metody HTTP, minimalnie GET, POST, PUT, PATCH
 - c) nagłówek Authorization
 - d) dodatkowych nagłówek zawierających adres IP atakującego, MAC adres atakującego.
- 20) System musi umożliwiać wgranie własnych licencji posiadanych przez Zamawiającego na systemy pułapki z systemem Windows.
- 21) System musi umożliwiać wgranie własnych spersonalizowanych obrazów dla systemów Windows 10, Windows 2016/2019/2022, umożliwiając:
- a) dołączenie pułapki do Active Directory
 - b) włączenie usług takich jak SQL i http
 - c) wykorzystanie poświadczeń AD jako przynęty, w celu uzyskania dostępu do usług, np. RDP/SSH, wykrywając przejęte konta z Active Directory
- 22) System musi umożliwiać wgranie własnego spersonalizowanego obrazu dla systemu Red Hat Enterprise Linux i Ubuntu
- 23) System musi umożliwiać ściągnięcie lub eksport danych takich jak:
- a) ruch generowany przez atakującego jako plik PCAP
 - b) zdarzenia IDS oraz stron www, które odwiedzał atakujący z pułapki
- 24) Powyższe dane muszą być możliwe do eksportu w postaci danych IOC do konsumpcji przez inne platformy w formacie minimalnie CSV i w integracji z systemami STIX/TAXII.
- 25) System musi integrować się z systemem VirusTotal w celu wysłania hash pliku i integracji wyniku skanowania w incydencie.
- 26) System musi integrować się z systemami dynamicznej analizy plików (sandbox), minimalnie z Cuckoo Sandbox.
- 27) System musi integrować się z systemem SIEM.
- 28) System musi integrować się z systemami SIEM w taki sposób, że wysyłane są do nich utworzone na pułapkach dane dostępowe (login).

- 29) System musi wysyłać zdarzenia z wykorzystaniem SYSLOG oraz wspierać format Common Event Format (CEF). Musi też istnieć możliwość wysyłania komunikatów syslog w postaci zaszyfrowanej.
- 30) System musi umożliwiać wykrywanie istniejących zasobów poprzez pasywne wykrywanie systemów operacyjnych, zasobów OT/IT/IoT w danej sieci optymalizując implementacją pułapek.
- 31) System musi wspierać konfiguracje białych list, adresów IP oraz zakresów adresów IP razem ze źródłowymi i docelowymi portami w połączeniu z konkretnymi przynętami/usługami oraz pułapkami, które nie będą podlegały wykrywaniu w celu minimalizacji fałszywych alarmów. Konfiguracja musi umożliwiać wskazanie czy dla danego adresu/zakresów adresów IP system nie będzie generował incydentów, czy też będzie blokował ruch z danego adresu/zakresów adresów IP
- 32) System musi umożliwiać centralne zarządzanie dostarczonych zdalnych systemów deceptyjnych w ramach tego postępowania.
- 33) System musi wspierać uruchomienie centralnego zarządzania na istniejącym i działającym systemie deceptyjnym z uruchomionymi pułapkami/przynętami.
- 34) System musi wspierać konfigurację VLAN trunking.
- 35) System musi wspierać automatyczne wykrywanie VLANów,
- 36) System musi wspierać wykrywanie zasobów oraz działających usług na wskazanych interfejsach poprzez pasywne rozpoznawanie tych systemów oraz usług. Wynikiem działania wykrywania musi być lista zawierająca minimalnie:
 - a) Adres IP systemu/urządzenia
 - b) MAC systemu/urządzenia
 - c) Producent systemu/urządzenia
 - d) Podsieć/interfejs na którym system został wykryty system/urządzenie
 - e) Nazwę systemu/urządzenia
 - f) Wykryty system operacyjny
 - g) Wykryty firmware systemu/urządzenia
 - h) Typ wykrytego systemu/urządzenia
- 37) System musi wspierać implementacje w środowisku całkowicie odizolowanym od Internetu (air-gap).
- 38) System musi być zarządzany przez webową stronę, połączenie realizowane z wykorzystaniem protokołu HTTPS.
- 39) System musi umożliwiać dostosowanie dashboardu zarządzającego w oparciu o predefiniowane widżety.

- 40) System musi umożliwiać monitorowanie po SNMP, wsparcie minimalnie dla wersji V2c i V3. System musi oferować pakiet MIB.
- 41) System musi umożliwiać wysyłanie zdarzeń oraz raportów z wykorzystaniem poczty.
- 42) System musi umożliwiać konfiguracje dostosowanych zdarzeń, które zostaną wysłane drogą pocztową.
- 43) System musi umożliwiać eksport raportów w formacie PDF i CSV.
- 44) System musi udostępniać własne API umożliwiające minimalnie:
 - a) Otrzymanie listy wzorców do opublikowania pułapki/przynęty
 - b) Opublikowanie pułapki/przynęty na podstawie wybranego wzorca
 - c) Otrzymanie statusu w jaki znajduje się pułapka/przynęty
 - d) Możliwość zatrzymania i wystartowania pułapki/przynęty
 - e) Otrzymanie wygenerowanych incydentów z możliwością filtrowania per zakres czasowy i nazwę pułapki/przynęty
- 45) System musi umożliwiać dostosowanie komunikatu po zalogowaniu (Login Disclaimer).
- 46) System musi wspierać zewnętrzne metody uwierzytelniania użytkowników do systemu, nie mniej niż:
 - a) LDAP
 - b) RADIUS
 - c) SAML
- 47) System musi wspierać silne uwierzytelnienie.
- 48) System musi wspierać konfiguracji kont dostępowych z wykorzystaniem ról (RBAC)
- 49) System musi umożliwiać konfigurację własnych profili ról.
- 50) Rozwiązanie musi umożliwiać użytkownikom wymianę informacji o wykrytych i zidentyfikowanych lokalnie technikach ataku z innymi użytkownikami. Dzięki takiej opcji współpracy w społeczności zorganizowanej w ramach funkcjonalności realizowanej przez producenta platformy możliwe będzie wykrywanie i unikanie ataków prowadzonych według schematu, który został wykryty przez innego klienta. System musi posiadać publicznie dostępną dokumentację, utrzymywaną i udostępnianą przez producenta, co najmniej w zakresie:
 - a) Dokumentacja administratora systemu – w zakresie konfiguracji systemu. Powinna zawierać przykłady konfiguracji
 - b) Dobre praktyki – w zakresie zaleceń najlepszych praktyk podczas konfiguracji systemu

- c) Dokumentacja instalacyjny – w zakresie instalacji i pierwszej konfiguracji
- d) Informacje o nowych wersjach (release notes) – w zakresie zmian wprowadzonych w oprogramowaniu, nowych funkcjach, usuniętych problemach
- e) Aktualizacja systemu – w zakresie procedur postępowania przy zmianie wersji oprogramowania
- f) Własne zmiany obrazu pułapki – w zakresie możliwości i sposobu dopasowania pułapki tak aby odzwierciedlała rzeczywiste maszyny występujące w środowisku użytkownika
- g) Filmy instruktażowe – prezentacja audio-wizualna wykonywania podstawowych zadań konfiguracyjnych, np. uruchomienie pułapki konkretnego typu
- h) Forum użytkowników systemu.

4. Serwisy i licencje

- 1) W ramach zamówienia mają zostać dostarczone:
 - a) Centralny system sprzętowy (maszyna główna) który będzie realizował zarówno tworzenie pułapek jak i zarządzanie zdalnymi urządzeniami – 1 sztuka;
 - b) Zdalne urządzenia, zarządzane centralnie, do tworzenia lokalnych pułapek – 4 sztuki
- 2) W ramach zamówienia mają zostać dostarczone subskrypcje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów przez okres 36 miesięcy. Powinny one obejmować:
 - a) System musi wspierać umieszczenie systemów pułapek i przynęt w minimum 14 podsieciach z maską sieciową /24 bity.
 - b) Wymaga się dostawy licencji na systemy operacyjne do pracy z minimum 8 maszynami wirtualnymi Microsoft Windows 10 jako pułapki utrzymywane przez producenta rozwiązania.
 - c) Dostarczona licencja na system musi umożliwiać uruchomienie wszystkich pułapek i przynęt wskazanych w punkcie 3.5. sekcji „Funkcje szczegółowe systemu ochrony”, z wykluczeniem licencji na same systemy operacyjne, jeżeli tego wymagają.

5. Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy. W ramach licencji producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

W wypadku awarii i konieczności wymiany sprzętu należy zapewnić, iż trwałe nośniki informacji jak dyski pozostają w siedzibie Zamawiającego.

Część 4 System uwierzytelniania, autoryzacji i kontroli dostępu

Dostawa, instalacja oraz serwis systemu uwierzytelniania, autoryzacji i kontroli dostępu.

Wykonawca musi przedłożyć oświadczenie producenta lub autoryzowanego partnera producenta, że Wykonawca posiada autoryzację producenta lub autoryzowanego partnera producenta w zakresie sprzedaży oferowanego rozwiązania.

Szczegółowe wymagania opisano w tabeli poniżej.

L p.	Parametr	Wymagania techniczne
1.	Architektura systemu	Dostarczony system uwierzytelniania musi zapewniać wszystkie wymienione poniżej funkcje. Oferowane rozwiązanie musi pozwalać na centralne zarządzanie kontami użytkowników i ich uwierzytelnianiem. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta.
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa.
3.	Parametry fizyczne systemu	1. System musi być dostarczony w formie klastra wysokiej dostępności (ang: High Availability) w oparciu o rozwiązanie sprzętowe, co najmniej dwa urządzenia. Każde z urządzeń musi posiadać: a. Dyski w konfiguracji niezawodnościowej b. Redundantne zasilacze c. Cztery interfejsy Ethernet 10/100/1000 Urządzenia muszą pochodzić od tego samego producenta co oprogramowanie na nim zainstalowane.
4.	Wymagania ogólne	1. System powinien pozwalać na nie mniej niż: a. zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrznej konsoli zarządzającej b. możliwość pracy w konfiguracji HA (High Availability)

		<p>z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności</p> <p>c. odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż):</p> <ul style="list-style-type: none"> • obciążenia procesor(a/ów) • wykorzystania pamięci • obciążenia dysku • zmiany adresu IP interfejsu • informacji o osiągnięciu granicznej liczby użytkowników • informacji o osiągnięciu granicznej liczby grup użytkowników • przekroczeniu liczby uwierzytelnień • przekroczeniu liczby błędnych uwierzytelnień • zmiana stanu HA <p>d. graficzną reprezentację statusu uwierzytelnień</p> <p>e. logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:</p> <ul style="list-style-type: none"> • lokalnie • zdalnie w oparciu o protokół syslog <p>f. aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI)</p> <p>g. tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI)</p> <ul style="list-style-type: none"> • również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określeniem godzin i minut • rzeczona kopia bezpieczeństwa może również być również zapisywana przy pomocy protokołu FTP/SFTP • szyfrowanie kopii bezpieczeństwa <p>h. konfigurację captive portal</p>
5.	Wymagania funkcjonalne - uwierzytelnia	<p>1. Celem realizacji funkcji uwierzytelniających, system powinien wspierać nie mniej niż:</p> <p>a. lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania nie mniej niż następujących</p>

nie	<p>akcji na użytkownika: tworzenie, przypisanie tokena i zarządzanie nim, blokowanie konta (locking), usuwanie</p> <p>b. przechowywanie następujących informacji o użytkowniku: nazwa (username), imię/nazwisko, adres email, numer telefonu komórkowego, numer telefonu, adres, kraj, stan/województwo</p> <p>c. możliwość przechowywania przynajmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników</p> <p>d. możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV</p> <p>e. konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:</p> <ul style="list-style-type: none"> • poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych) • czasu życia hasła • możliwości ponownego użycia tych samych haseł <p>f. konfigurowalną politykę blokowania kont:</p> <ul style="list-style-type: none"> • w oparciu o ilość nieudanych logowań • czas blokowania • okres nieaktywności po którym konto jest blokowane <p>g. możliwość odzyskiwania haseł:</p> <ul style="list-style-type: none"> • z wykorzystaniem adresu email • z wykorzystaniem pytania pomocniczego <p>h. uruchomienie portalu do samodzielnej rejestracji użytkowników</p> <ul style="list-style-type: none"> • opcjonalnie tworzenie ich kont może wymagać akceptacji administratora • wymagana jest również opcja tworzenie kont bez ingerencji administratora <p>i. obsługę protokołu RADIUS zgodną z RFC</p> <ul style="list-style-type: none"> • wbudowany serwer RADIUS • konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS • integrację z zewnętrznymi serwerami RADIUS
-----	---

		<ul style="list-style-type: none"> • możliwość importowania użytkowników RADIUS z zewnętrznego serwera LDAP j. obsługę protokołu TACACS+ • konfiguracja serwera pozwala na ograniczenie dostępu tylko dla wskazanych klientów • możliwość importowania klientów z pliku CSV oraz przy pomocy API • specyfikowanie listy dozwolonych/blokowanych poleceń powłoki i usług k. obsługę protokołu LDAP • wbudowany serwer LDAP • możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP) l. obsługę SAML - Identity Provider (IdP) proxy ł. realizację funkcjonalności SSO (Single Sign On) w oparciu o: <ul style="list-style-type: none"> • integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny • dedykowaną aplikację na stację robocze z systemem Windows • RADIUS • informacje uzyskiwane poprzez protokół syslog • dedykowany portal m. możliwość wykorzystania dodatku plug-in do
6.	Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe	<p>1. Realizując uwierzytelnianie dwuskładnikowe, system musi spełniać nie mniej niż:</p> <p>a. obsługę dla tokenów sprzętowych (hardware):</p> <ul style="list-style-type: none"> • ich działanie musi być realizowane w oparciu o protokół OAuth wraz ze wsparciem dla TOTP oraz HOTP • wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania <p>b. wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android.</p> <p>c. dla tokenów na system iOS i Android wymaga się:</p>

		<ul style="list-style-type: none"> • aktywacji z centralnego systemu uwierzytelniania (seed provisioning) • możliwości konfiguracji ilości generowanych cyfr (6 lub 8) • generowania kodu (cyfr) co 30 lub 60 sekund • możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne) • ochrony dostępu poprzez konfigurowalny kod PIN • aktywacji w oparciu o kod QR • możliwość przypisania własnego logotypu organizacji widocznego w aplikacji tokena mobilnego <p>d. możliwość dostarczenia kodu (wskazania tokena) poprzez:</p> <ul style="list-style-type: none"> • email (wygaśnięcie kodu w czasie 10-3600 sekund) • SMS (wygaśnięcie kodu w czasie 10-3600 sekund) <ul style="list-style-type: none"> ▪ konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP <p>e. w przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem"</p> <p>f. możliwość integracji z logowaniem do systemu Windows</p> <p>g. wsparcie dla API</p>
--	--	--

7.	Wymagania funkcjonalne - 802.1x	<p>1. System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:</p> <p>a. dla sieci bezprzewodowych wymagane są następujące protokoły:</p> <ul style="list-style-type: none"> • PEAP • EAP-TTLS • EAP-TLS • EAP-GTC <p>b. wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication)</p> <p>c. zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP</p> <p>d. możliwość samodzielnej rejestracji urządzeń przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów</p>
8.	Wymagania funkcjonalne - zarządzanie certyfikatami	<p>1. System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:</p> <p>a. własne, samodzielne CA (Certificate Authority)</p> <p>b. CA pośredniczące (intermediary CA)</p> <p>c. ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego</p> <p>d. możliwość pobrania wygenerowanych certyfikatów</p> <p>e. możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP</p> <p>f. możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP</p> <p>g. możliwość generowania certyfikatów typu wildcard</p> <p>h. realizacja CRL (Certificate Revocation List)</p> <p>i. wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560)</p>

9.	Maksymalne parametry wydajnościowe	<p>1. Każde urządzenie musi mieć możliwość obsługi co najmniej:</p> <ul style="list-style-type: none"> a. uwierzytelnianie dla 18 000 użytkowników b. 15 000 tokenów (uwierzytelnianie dwuskładnikowe) c. 6 000 klientów protokołu RADIUS (urządzeń NAS) d. 800 grup użytkowników e. 50 certyfikatów głównych (CA) f. 40 000 certyfikatów użytkowników
10.	Parametry wydajnościowe i licencyjne	<p>Wymaga się, aby dostarczony klaster obsługiwał co najmniej:</p> <ul style="list-style-type: none"> a. uwierzytelnianie dla 4 000 użytkowników <p>Wraz z urządzeniami należy dostarczyć kompatybilne tokeny tego samego producenta:</p> <ul style="list-style-type: none"> b. 3000 tokenów w formie aplikacji na telefon (uwierzytelnianie dwuskładnikowe) c. 100 tokenów sprzętowych
11.	Zarządzanie	<p>System udostępnia:</p> <ul style="list-style-type: none"> • Graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS • Interfejs REST API
12.	Serwisy, szkolenia i usługi	<p>Wymaga się, aby dostawa obejmowała również serwis producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.</p> <p>Uszkodzone dyski muszą pozostać w siedzibie Zamawiającego.</p>

Zamówienie dofinansowane ze środków Unii Europejskiej, Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności; Inwestycja: C3.1.1. Cyberbezpieczeństwo - CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; Cyberbezpieczeństwo - Cyberbezpieczny Rząd – w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, na podstawie porozumienia o powierzenie grantu o numerze KPOD.05.10- CR.01-001/24/0036/ KPOD.05.10-CR.01-001/25/2025"