Załącznik .....

OPIS PRZEDMIOTU ZAMÓWIENIA

Usługi monitorowania Security Operations Center

I.	**Przedmiot zamówienia**	
1	Przedmiotem zamówienia jest zakup usługi SOC wraz z wdrożeniem systemu SIEM w infrastrukturze Zamawiającego w celu zwiększenia poziomu Cyberbezpieczeństwa infrastruktury IT Zamawiającego przez okres 36 miesięcy od dnia podpisania protokołu zdawczo-odbiorczego nie wcześniej niż 20.03.2026, jednak nie później niż do dnia 30 kwietnia 2026.	
2	Usługa obejmuje świadczenie monitorowania i reagowania na incydenty bezpieczeństwa w trybie 24/7/365 przez dedykowany zespół wykonawcy w okresie obowiązywania umowy. W ramach usługi dostarczony zostanie system klasy SIEM, zintegrowany z infrastrukturą Zamawiającego, obejmującą m.in. Active Directory, systemy backupu, systemy operacyjne oraz urządzenia sieciowe.	
3	Monitorowanie w trybie ciągłym systemów teleinformatycznych oraz sieci Zamawiającego (SOC). Usługa świadczona za pomocą narzędzi Wykonawcy, przez jego zespół w zakresie cyberbezpieczeństwa, zgodnie z wymaganiami Rozporządzenia 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 (Dz.U. z 2019 r. poz. 2479).	
4	Przedmiot Zamówienia będzie realizowany w oparciu o przygotowany uprzednio przez Wykonawcę harmonogram ramowy, który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić harmonogram ramowy w terminie 7 dni od daty podpisania umowy.	
5	Wykonawca w harmonogramie ramowym musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.	
6	Wymaga się, aby Wykonawca przygotował harmonogram wdrożenia uwzględniający etapy wdrożenia: - analiza przedwdrożeniowa, - instalacja, konfiguracja systemu i dostrojenie systemu, - szkolenia i dokumentacja powdrożeniowa.	
II.	**Wymagania dla usługi Security Operations Center (SOC)**	
1	W ramach realizacji przedmiotu zamówienia Wykonawca będzie monitorował i reagował na incydenty na podstawie logów udostępnionych przez Zamawiającego.	
2	W ramach obowiązków Wykonawcy będzie wykonanie następujących czynności:	

	- dostarczenie systemu klasy SIEM w modelu usługowym - monitoring oraz segregacja incydentów, zdarzeń i anomalii - obsługa incydentów w zakresie scenariuszy obsługi, w tym kategoryzację i priorytetyzacją incydentów, - analiza incydentów zgodnie z ustalonymi z Zamawiającym procedurami i scenariuszami - weryfikacja incydentów wygenerowanych w dostarczonym systemie oraz ich analiza w systemach bezpieczeństwa Zamawiającego.	
3	W ramach realizacji zadań Wykonawca przygotuje i wdroży możliwe scenariusze wystąpienia incydentów bezpieczeństwa w systemie SIEM, które zostaną zaakceptowane przez Zamawiającego. Przykładowe scenariusze, które obligatoryjnie powinny być zaimplementowane: - bruteforce attack (atak siłowy), - atak złośliwego oprogramowania (malware), - atak typu DDoS, - wykrywanie usług sieciowych (Network Service Discovery), - zdalne wykrywanie systemów (Remote System Discovery), - pozyskiwanie informacji o systemie (System Information Discovery), - interpreter poleceń i skryptów (Command and Scripting Interpreter), - file integrity monitoringu (FIM) kluczowych plików konfiguracyjnych, - detekcja anomalii oraz detekcja zagrożeń klasy rootkit	
4	W ramach realizacji zadań Wykonawca przygotuje i wdroży scenariusze reakcji rozumiane jako zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz reakcji powinien składać się z podzadań realizujących funkcje: - wzbogacenia wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez udostępnione narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji, - analizy zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu - wydanie rekomendacji działań rozumianej jako zestawienie rekomendacji umożliwiających ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym, - informowania i raportowania obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.	
5	W ramach usługi SOC Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, w tym z wykorzystaniem technik inżynierii odwrotnej (ang. reverse engineering), w wymiarze min 12 w ciągu roku (kryterium oceny ofert). Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:	

	- analiza statyczna wskazanej próbki złośliwego oprogramowania, - analizy dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy, - proces odwrotny do obfuskacji umożliwiający analizę kodu zaciemnionego, - analiza występowania modułów pozwalających na kontrolę w tym szczegółowego określenia zaimplementowanych funkcji, - w przypadku wykorzystywania rodziny malware określenia wersji. Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca przekaże drogą mailową raport z wykonanej analizy.	
6	W ramach realizacji zadań Wykonawca będzie świadczył usługę administracji systemem SIEM obejmującą: - informowanie Zamawiającego o awariach Systemu SIEM, mogących uniemożliwić poprawne działanie systemów informacyjnych, Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie, - rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa, - optymalizowanie konfiguracji Systemu SIEM w celu nieprzekraczania wartości licencji niezbędnej do obsługi incydentów generowanych w infrastrukturze Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji, - konfigurację Systemu SIEM w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego w Analizie Przedwdrożeniowej, - weryfikację czy System SIEM prawidłowo analizuje logi, - tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.	
7	Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.	
8	Za podjęcie incydentu uważa się reakcję operatora polegającą na przeniesieniu incydentu w stan segregacji oraz rozpoczęcie działań zmierzających do wyjaśnienia zaistniałego incydentu.	
9	W ramach usługi SOC Zamawiający wymaga, aby Wykonawca minimum raz w miesiącu przeprowadził spotkanie (Zamawiający dopuszcza formę zdalnego spotkania), na którym będą przedstawione oraz omówione najczęściej występujące zdarzenia wraz z propozycjami dostosowania rozwiązania SIEM celem ograniczenia występowania incydentów False Positive, czyli gdy wykryto atak lub zagrożenie, podczas gdy nie miały one miejsca.	
10	Wykonawca gwarantuje informowanie Klienta (za pośrednictwem ustalonych w umowie kanałów komunikacji (telefon/e-mail/portal zgłoszeń) o wykrytych incydentach krytycznych w ciągu 30 minut oraz o wykrytych innych incydentach w ciągu 4 godzin od momentu ich wykrycia wraz z informacją o podjętych działaniach.	
11	Zamawiający wymaga, aby każdy miesiąc świadczenia Usług podsumowany został raportem miesięcznym. Wykonawca zobowiązany jest przedstawić raport w terminie 5 dni roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa. Raport ten powinien zostać wysłany na adres poczty elektronicznej wskazany w treści umowy,	

	Opis incydentu powinien składać się z sekcji: - monitorowanie cyberbezpieczeństwa: - data świadczenia usług, - zestawienie obsłużonych incydentów, - identyfikator incydentu, - nazwa, - klasyfikacja priorytetu Incydentu, - dokładna data i godzina ujawienia incydentu, - statusy końcowe, - ogólne rekomendacje i zalecenia dla Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.	
12	Wykonawca zobowiązuje się do realizowania czynności w następujących terminach: a) podjęcie reakcji do 30 minut od momentu wystąpienia zdarzenia/incydentu, b) Czas realizacji na incydent krytyczny – do 2 godzin, c) Czas realizacji na incydent niekrytyczny – do 12 godzin, d) Czas realizacji na false positive – do 24 godzin.	
13	W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie SIEM w ramach wsparcia w trybie 24/7/365, 7 dni w tygodniu.	
14	Wsparcie będzie odpowiedzialne za: - dostępność usługi dla Zamawiającego - monitorowanie zdarzeń naruszenia cyberbezpieczeństwa - analizę zgłoszonych Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń po incydentalnych, - przygotowanie miesięcznych raportów z realizacji prac, - przygotowanie, wdrożenie i realizacja Scenariuszy Reakcji dla zidentyfikowanych zagrożeń (playbooki), - dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji, - udostępnienie, administrowanie i utrzymanie systemu Security Incident and Event Management oraz integracja ze źródłami logów podmiotu, takimi jak Active Directory, Serwery Windows i Linux, DNS, system antywirusowy, WAF, Firewall, IPS / IDS, VPN, Routery i przełączniki, - wspieranie personelu Zamawiającego we wdrożeniach rekomendacji po wystąpieniach incydentów, - wspieranie personelu Zamawiającego w zakresie wprowadzania zmian konfiguracyjnych w systemach IT oraz rozwiązaniach bezpieczeństwa w celu zapewnienia i utrzymania odpowiedniego poziomu bezpieczeństwa. - łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa, - zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive), - priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa, - modyfikacja polityk bezpieczeństwa systemów, aplikacji, rozwiązań podmiotu celem dostosowania ich do skuteczniejszego wykrywania zagrożeń (tuning systemów bezpieczeństwa), - monitorowaniem muszą zostać objęte kluczowe: a) stacje robocze oraz serwery	

	b) urządzenia sieciowe, w tym urządzenia brzegowe, c) systemy / aplikacje serwerowe, w tym systemy informacji medycznej, d) kontrolery domenowe, e) środowiska chmurowe wraz z aplikacjami – o ile są wykorzystywane - zakres monitorowanych zdarzeń powinien uwzględniać minimum: a) powiadomienia o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowane z narzędzi ochrony, b) powiadomienia o dezaktywacji narzędzi bezpieczeństwa na danym hoście, c) powiadomienia z modułów ochrony / bezpieczeństwa urządzeń brzegowych oraz wewnętrznych urządzeń sieciowych, d) zdarzenia dotyczące nieudanych, wielokrotnych prób logowania dla wszystkich monitorowanych aktywów, e) kluczowe zdarzenia (np. utworzenie konta, zmiana hasła, usunięcie konta, zmiana grupy) związane z kontami uprzywilejowanymi dla wszystkich monitorowanych aktywów, f) zdarzenia sieciowe oraz systemowe (np. enumeracja, skanowanie portów i adresacji) mogące świadczyć o rekonesansie infrastruktury, g) zdarzenia związane z modyfikacją mechanizmów harmonogramu w systemach operacyjnych, h) zdarzenia związane z modyfikacją audytu zdarzeń / dzienników systemowych, i) zdarzenia dotyczące integralności plików, w szczególności zasobów sieciowych mogące świadczyć o zainfekowaniu oprogramowaniem złośliwym, j) zdarzenia związane z logowaniem zdalnym.	
15	Czas podjęcia Incydentu będzie liczony jako różnica czasu pomiędzy odnotowaniem wystąpienia zdarzenia a czasem nadania priorytetu. Zamawiający wyróżnia trzy poziomy incydentów: Krytyczny, niekrytyczny, False Positive zgodnie z poniższym zestawieniem: Krytyczny: a) Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; b) Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicator of Compromise (pol. Wskaźnika skompromitowania); c) Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); d) Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; e) Informacja o potencjalnym cyberzagrożeniu od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; f) Potwierdzona informacja o potencjalnym cyberzagrożeniu od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; g) Informacja o potencjalnym cyberzagrożeniu od Dyrektora lub Kierownika Departamentu Bezpieczeństwa;	

	h) Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; i) Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; j) Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej; k) Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego KSC lub RODO; a) Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); b) Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; Niekrytyczny a) Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego Indicators of Compromise (pol. Wskaźnika skompromitowania) na systemie chronionym; b) Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; c) Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; d) Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa; e) Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie; False Positive Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.	
16	Zamawiający wymaga każdorazowo po wystąpieniu Incydentu o priorytecie Krytycznym Raportu Po incydentalnego nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje: - unikalny identyfikator zdarzenia, - kiedy incydent wystąpił? - kiedy incydent został zauważony / wykryty? - jaki proces był sprawcą incydentu? - co się wydarzyło? - gdzie wydarzenie miało miejsce? - dlaczego zdarzenie mogło wystąpić?	

	- jakie czynności powinny zostać przeprowadzone przez Zamawiającego w celu powstrzymania incydentu? - wspieraniu personelu Zamawiającego we wdrożeniach rekomendacji po wystąpieniach incydentów.	
17	Wykonawca zobowiązany jest do przeprowadzenia testów penetracyjnych infrastruktury Zamawiającego w modelu grey-box/white-box, w tym zewnętrznych i wewnętrznych testów sieciowych i aplikacji zgodnie z metodykami OWASP Top 10 i PTES przynajmniej raz w roku. Raport z testów będzie zawierał opis metodologii, dowody (zrzuty ekranu, logi) oraz rekomendacje naprawcze z priorytetyzacją (krytyczne/wysokie/średnie/niskie). Po załataniu podatności możliwość przeprowadzenia re-testów.	
18	W ramach usługi SOC Wykonawca będzie wysyłał Zamawiającemu informacje odnośnie pojawiających się podatności dla systemów wskazanych w ramach podłączonych źródeł logów nie rzadziej niż raz na miesiąc.	
	III. Wymagania dotyczące wdrożenia	
1	System SIEM/SOAR musi być dostarczony, wdrożony i zainstalowany: - po stronie Zamawiającego na udostępnionej maszynie wirtualnej zainstalowane zostaną stosowne kolektory danych umożliwiające zbieranie logów, które będą podlegały analizie, - po stronie Wykonawcy zainstalowana będzie centralna instancja wykorzystywana do analizy i generowania zdarzeń lub anomalii oraz obsługi zdarzeń i incydentów.	
2	Wykonawca w ramach pierwszego etapu dokona analizy przedwdrożeniowej obejmującej wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie rozwiązania SIEM w środowisku informatycznym Zamawiającego. Analiza musi zawierać w szczególności: 1. dane wstępne: plan i sposób komunikacji Stron, harmonogram wdrożenia, 2. informacje o systemach bezpieczeństwa: analiza stanu bezpieczeństwa użytkowanych systemów przed rozpoczęciem realizacji projektu oraz opis koniecznych działań dla osiągnięcia wymaganego stanu cyberbezpieczeństwa.	
3	Wykonawca w ramach drugiego etapu zainstaluje zaoferowane oprogramowanie według wcześniej przedstawionej architektury działania rozwiązania oraz wcześniej przygotowanego schematu komunikacji sieciowej w sieci lokalnej Zamawiającego. Zaimplementuje/skonfiguruje opracowane przez producenta reguły bezpieczeństwa wraz z weryfikacją ich działania dla konkretnych procesów określonych na etapie analizy przedwdrożeniowej. Dostroi system tak, aby nie powodował nadmiernej ilości fałszywych alarmów zaciemniających realne możliwe zagrożenia. Nie dopuszcza się sytuacji, w której jedno źródło logów spowoduje destabilizację działania całego systemu SIEM w krótkim okresie czasu np. 10 minut.	
4	Wykonawca w ramach trzeciego etapu przeprowadzenie szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów oraz sporządzi i przekaże dokumentację powdrożeniową wskazującą wszystkie istotne elementy z punktu widzenia wdrożenia, wraz ze wszystkimi danymi dostępowymi do ewentualnych kont technicznych stworzonych na etapie wdrożenia oraz wykaz przygotowanych scenariuszy reagowania na wykryte incydenty.	

	IV. Zakres systemów Zamawiającego objętych usługą SOC	
1	Monitorowaniu będzie podlegać minimum: 1100 szt. stacji roboczych (windows) 40 szt. serwerów fizycznych i macierzy 100 szt. serwerów wirtualnych (linux / windows) 10 szt. urządzeń sieciowych (hpe / huawei / extreme network) 26 szt. systemów wirtualizacyjnych (hyper-v / vmware / proxmox / H3C KVM) 6 szt. systemów bezpieczeństwa (eset / fortinet / extreme networks) 128 szt. adresacja publiczna Zamawiającego 2 szt. dedykowane serwery usług pocztowych i hostingowych (w zewnętrznej infrastrukturze po za siecią Zamawiającego)	
	V. Wymagania funkcjonalne w zakresie zarządzania podatnościami	
1	- cykliczna identyfikacja oraz analiza podatności dla systemów lokowanych w sieci Zamawiającego, - dobowa identyfikacja oraz analiza podatności dla systemów Zamawiającego lokowanych w sieci publicznej, - monitoring zewnętrzny publicznej klasy adresowej w zakresie zmian eksponowanych usług, - opracowywanie rekomendacji dla zidentyfikowanych podatności, - dostarczanie rekomendacji dla zidentyfikowanych podatności w formie dostępu do systemu teleinformatycznego Wykonawcy, - monitorowanie oraz wspieranie w przypadku braku możliwości wdrożenia rekomendacji.	
	VI. Wymagania funkcjonalne w zakresie architektury bezpieczeństwa	
1	- nadzór nad rozwojem utrzymywanego modelu bezpieczeństwa teleinformatycznego, - opracowywanie cyklicznych rekomendacji dot. modelu bezpieczeństwa na podstawie informacji i ryzyk pozyskanych w ramach obsługi incydentów bezpieczeństwa, - wspieranie w opracowywaniu wymagań bezpieczeństwa dla wdrażanego oprogramowania, - wspieranie w interpretacji wymagań prawnych odnoszących się do bezpieczeństwa teleinformatycznego w zakresie kompletności utrzymywanego modelu bezpieczeństwa.	
	VII. Wymagania funkcjonalne w zakresie systemu SIEM	
1	1. System przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.	
2	System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.	
3	Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać zainstalowania dedykowanego oprogramowania bezpośrednio na tych systemach.	
4	System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od	

	zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.	
5	System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.	
6	System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.	
7	System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników: a) fqdn, b) e-mail, c) nazwa pliku, d) ścieżka do pliku, e) hash, f) adres IP, g) klucz rejestru, h) cmd.	
8	System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie np. MISP.	
9	Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).	
10	System musi umożliwiać integrację z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, jednostkę organizacyjną.	
11	System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.	
12	System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności (np.: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).	
13	System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).	
14	System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.	
15	System musi umożliwiać gromadzenie i korelację zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.	
16	Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą	

	regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: a) adresie IP, b) koncie domenowym użytkownika, c) strefie bezpieczeństwa, d) zakresie adresów IP.	
17	Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop" umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.	
18	System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.	
19	Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in. a) wszystkie skorelowane zdarzenia, b) korespondencja pocztowa, c) załączniki z próbkami lub dowodami, d) wskaźniki kompromitacji (IoC), e) informacje pozyskane z innych systemów.	
20	Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: a) nazwy zasobu, b) rodzaju zasobu, c) ważności zasobu dla organizacji, d) rodzaj przetwarzanych informacji, e) usług, które ten zasób świadczy, f) lokalizację użytkowników, którzy z niego korzystają, g) usługi, z których zasób korzysta.	
21	System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.	
22	Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.	
23	Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów (udostępniany tylko na prośbę Zamawiającego).	
24	W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.	
25	Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: a) wybór raportu, który ma zostać wysłany, b) zdefiniowanie jego tytułu, c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d) możliwość ograniczenia cyklu do dni powszednich, e) określenie daty przesłania pierwszego raportu, f) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do: · zdefiniowanej daty końcowej, · określonej liczby raportów, g) określenie odbiorców raportu.	

26	System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).	
27	System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard'u", tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.	
28	System musi pozwalać na tworzenie dedykowanych dashboardów obejmujących: a) zestaw wykresów dla bieżącego użytkownika, b) zestaw wykresów dla wybranego użytkownika, c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).	
29	Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji.	
30	Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.	
31	Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)	
32	Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.	
33	Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log) / danych znormalizowanych.	
34	System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Intelligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.	
35	System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal.	
36	System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.	
37	W związku z tym, że obsługa systemu po stronie Zamawiającego ma objąć także użytkowników nie posługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.	
38	Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.	
39	Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać min. **1400** źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.	
40	System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.	

VIII.	**Wymagania funkcjonalne w zakresie systemu SOAR**	
1	System SOAR musi zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydent, które natywnie (tj. poprzez wbudowaną funkcjonalność i możliwości) w pełni integrują się z większością technologii bezpieczeństwa na rynku.	
2	System SIEM musi być kompatybilny z modułem obsługi incydentów SOAR.	
3	System SIEM i SOAR muszą umożliwić, autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność, a także zapewniać poufność transmisji danych.	
4	System SOAR musi zapewniać kontrolę wersji dostępnych scenariuszy (playbooks).	
5	System SOAR musi zapewniać uruchamianie scenariuszy automatycznych, półautomatycznych, manualnych.	
6	System SOAR musi zawierać wiele gotowych, dostępnych natywnie w systemie scenariuszy orkiestracji.	
7	System SOAR musi umożliwiać tworzenie przypomnień dla zadań.	
8	System SOAR musi oferować gotowe integracje z rozwiązaniami bezpieczeństwa dostępnymi na rynku. Gotowe integracje muszą zawierać przygotowane do użycia akcje.	
9	System SOAR musi umożliwiać współpracę pomiędzy analitykami bezpieczeństwa w czasie rzeczywistym	
10	Każdy incydent musi posiadać unikalny identyfikator,	
11	System SOAR musi mieć możliwość zmiany krytyczności incydentu w oparciu o zdefiniowane kryteria.	
12	System SOAR musi posiadać funkcjonalność zarządzania sprawami pozwalającą na rekonstrukcję wykonanych działań, podjętych decyzji, raportowania realizacji dochodzenia.	
13	System SOAR musi dostarczać raporty z możliwością ich dostosowania z wykorzystaniem pól z incydentu lub pól z własnym tekstem	
IX.	**Wymagania w zakresie usługi Managed Detection & Response (MDR)**	
1	W ramach usługi Zamawiający oczekuje, że Wykonawca obejmie szczególnym nadzorem i opieką system klasy XDR (ESET Inspect) wdrożony i utrzymywany przez Zamawiającego. Licencje i koszty systemu pozostają po stronie Zamawiającego.	
2	W ramach usługi Wykonawca będzie przez 1 godzinę dziennie monitorował i reagował na zdarzenia (detekcje) wyświetlane na podstawie logów udostępnionych przez Zamawiającego ze wskazanych źródeł oraz analizował zdarzenia bezpośrednio w konsoli ESET Inspect, w zakładce DETECTIONS.	
3	Monitorowane są w pierwszej kolejności zdarzenia (detekcje) krytyczne (czerwone) oraz ostrzegawcze (pomarańczowe).	

4	Zamawiający zapewni dostęp do połączenia bezpośredniego do konsol XDR ESET celu zapewnienia monitorowania.	
5	Wykonawca będzie na bieżąco przekazywał rekomendacje odnośnie dopracowania procesów bezpieczeństwa i działania infrastruktury IT Zamawiającego.	
6	Zamawiający informuje, że w trakcie umowy może nastąpić zmiana systemu bezpieczeństwa, aktualnie użytkowany ESET Protect może zostać zastąpiony innym oprogramowaniem. Zamawiający aktualnie posiada zainstalowanych 100 urządzeń z oprogramowaniem EDR, do końca 2026 roku będzie to 1100 urządzeń z oprogramowaniem EDR.	