Załącznik nr 3 do SWZ

	Wymagania funkcjonalne dla systemu SIEM	Oferowane parametry techniczne/funkcjonalności. Proszę wpisać Spełnia/Nie spełnia/, a jeśli nie spełnia podać jakie inne oferuje
1.	System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL.	
2.	System musi pracować w oparciu o architekturę Linux.	
3.	System musi mieć możliwość centralnego zbierania i zarządzania logami.	
4.	System działać w trybie zbliżonym do rzeczywistego.	
5.	System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.	
6.	Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.	
7.	System musi zapewniać efektywną obsługę co najmniej 100 GB danych dziennie.	
8.	System musi zapewniać retencję danych w okresie minimum 365 dni.	
9.	Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.	
10.	System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.	
11.	Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.	
12.	Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.	
13.	System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji.	
14.	System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu.	
15.	Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.	
16.	Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.	
17.	System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.	

18.	Interfejs musi posiadać angielską lub polską wersję językową.	
19.	System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).	
20.	Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.	
21.	Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius.	
22.	Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.	
23.	System musi wspierać mechanizm logowania typu Single Sign On.	
24.	System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.	
25.	System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.	
26.	System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.	
27.	System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.	
28.	System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.	
29.	System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.	
30.	System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.	
31.	System musi pozwalać na tworzenie parserów z poziomu GUI.	
32.	System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.	
33.	System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.	

34.	System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.	
35.	Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).	
36.	Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.	
37.	Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.	
38.	Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.	
39.	Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.	
40.	Oferowany system musi być wyposażony we wbudowany model językowy (LLM/GPT), dostarczony przez Producenta i stanowiący integralną część oferowanej platformy. Model językowy musi działać lokalnie w infrastrukturze Zamawiającego lub w środowisku chmurowym należącym do Producenta, z zapewnieniem zgodności z wymaganiami w zakresie bezpieczeństwa i ochrony danych obowiązującymi u Zamawiającego.	
41.	System musi umożliwiać integrację z zewnętrznymi modelami językowymi takimi jak OpenAI, Fireworks, lub modelem językowym (LLM) zgodnym ze standardem Ollama, z zachowaniem pełnej zgodności z zasadami bezpieczeństwa i ochrony danych obowiązującymi u Zamawiającego.	
42.	System musi umożliwiać definiowanie kontekstu organizacyjnego Zamawiającego, w tym:	

	wykorzystywanych technologii, struktury organizacyjnej oraz obowiązujących wymagań prawnych. Na podstawie wprowadzonych danych wbudowany model językowy (LLM) ma zapewniać generowanie wyników analizy dostosowanych do specyfiki działalności Zamawiającego.	
43.	Wbudowany model językowy (LLM), stanowiący integralną część oferowanego systemu, musi umożliwiać dynamiczną analizę gromadzonych danych, w szczególności w zakresie:	
	- automatycznego wyjaśnienia analizowanego zdarzenia,	
	- weryfikacji potencjalnego naruszenia bezpieczeństwa wraz z rekomendacją działań naprawczych,	
	- klasyfikacji wykrytego zagrożenia z wykorzystaniem matrycy MITRE ATT&CK,	
	- opisu wektora ataku,	
	- wykrycia naruszenia danych wrażliwych.	
44.	Oprogramowanie musi udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.	
45.	System musi umożliwiać rozbudowywanie funkcji Asystenta AI o nowe zapytania/prompty w kontekście analizy logów. Utworzone zapytania muszą być dostępne dla wszystkich użytkowników systemu za pomocą nowych przycisków lub pozycji list rozwijalnych.	
46.	Oprogramowanie powinno udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.	
47.	Oprogramowanie powinno udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.	
48.	Asystent AI musi pozwalać na budowanie odpowiedzi w dowolnym języku.	
49.	Asystent AI musi automatycznie dopasowywać zdarzenie do technik i taktyk matrycy MITRE.	
50.	Asystent AI musi dokonywać automatycznej izolacji obiektów IoC ze wskazanego rekordu logów.	

51.	System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.	
52.	System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.	
53.	Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.	
54.	System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.	
55.	System musi zapewniać parsowanie spływających do niego wiadomości w formatach:	
	- Syslog,	
	- WEF,	
	- Flat file,	
	- Event log,	
	- WMI,	
	- SNMP trap,	
	- XML,	
	- JSON,	
	- JDBC/ODBC	
	- CSV,	
	- Email.	
	Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.	
56.	System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.	
57.	System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.	
58.	System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.	
59.	System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.	
60.	Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.	

61.	System musi posiadać predefiniowany zestaw parserów zdarzeń.	
62.	System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta.	
63.	System musi wspierać geolokalizację zdarzeń na bazie adresów IP.	
64.	System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.	
65.	System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.	
66.	Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.	
67.	Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.	
68.	System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.	
69.	System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.	
70.	Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.	
71.	System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.	
72.	System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.	
73.	System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:	
	- wykrycia dowolnej treści w logach,	
	- wykrycia wystąpienia wartości pola na wybranej liście,	
	- wykrycia niewystępowania wartości pola na wybranej liście,	
	- wykrycia zmiany jednego z kilku pól,	
	- wykrycia zdarzeń występujących z zadaną częstotliwością,	

	- wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,	
	- wykrycia zaniku Wiadomości,	
	- wykrycia nowej wartości pola w zadanym okresie czasu,	
	- wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności.	
74.	System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów.	
75.	Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.	
76.	System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.	
77.	System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych.	
78.	System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności.	
79.	System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.	
80.	System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook.	
81.	System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.	
82.	Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.	
83.	System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.	
84.	Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).	
85.	System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.	
86.	System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.	

87.	System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule.	
88.	Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.	
89.	System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.	
90.	Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.	
91.	System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.	
92.	System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.	
93.	Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.	
94.	Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.	
95.	Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.	
96.	System musi umożliwiać zbieranie i analizę pełnego ruchu sieciowego (warstwy modelu ISO OSI od L2 do L7) oraz analizy formatu Netflow w wersji min. V5, v9 oraz IPFIX z wykorzystaniem oficjalnych modułów dostarczanych przez producenta.	
97.	System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, rentransmisji, Jitter, Server Response Time oraz Round Trip Time.	
98.	System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 1 roku.	
99.	Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.	
100.	System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.	
101.	Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.	
102.	Support producenta musi być świadczony w formule minimum 8/5.	
103.	Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.	

104.	Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.	
105.	System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.	
106.	System musi umożliwiać integrację z Mitre ATT@CK.	

	Lista źródeł	Oferowane parametry techniczne/funkcjonalności. Proszę wpisać Spełnia/Nie spełnia/, a jeśli nie spełnia podać jakie inne oferuje
1.	System musi zbierać i korelować logi z następujących źródeł:	
	- stacje robocze i serwery Windows (logi systemowe Windows Event Log),	
	- serwery Linux (dzienniki syslog),	
	- usługa Active Directory, Usługa federacyjna Active Directory (AD FS), usługi pocztowe (postfix, dovecot), usługi DNS (BIND), usługi WWW (Apache2, NGINX), bazy danych (MS SQL, PostgreSQL),	
	- rozwiązanie ESET Endpoint Antivirus/ESET Server Security,	
	- rozwiązanie WatchGuard EDR,	
	- VMware ESX,	
	- firewall WatchGuard,	
	- przełączniki sieciowe,	
	- zasilacze awaryjne (UPS).	
2.	Reguły korelacyjne, alerty i obsługa incydentów.	
3.	System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych.	
4.	System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.	
5.	System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.	
6.	System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.	

7.	System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów.	
8.	System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows.	
9.	System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP.	

	Wymagania funkcjonale dla systemu SOAR	Oferowane parametry techniczne/funkcjonalności. Proszę wpisać Spełnia/Nie spełnia/, a jeśli nie spełnia podać jakie inne oferuje
1.	Oprogramowanie musi wspomagać pracę zespołu reagowania na incydenty komputerowe (SOC, CERT, CSIRT, IRT itp.) tj. wspomagać procesy: monitorowania bezpieczeństwa teleinformatycznego, reagowania na incydenty, zarządzania podatnościami, gdzie głównym celem jest standaryzacja i automatyzacja działań analityków cyberbezpieczeństwa.	
2.	Oprogramowanie musi natywnie integrować się z systemem klasy SIEM wykorzystywanym przez Zamawiającego tj. producent oprogramowania SOAR musi oficjalnie wspierać integrację z dostarczanym rozwiązaniem SIEM.	
3.	Oprogramowanie musi umożliwiać automatyczne tworzenie incydentów wymagających obsłużenia na podstawie powiadomień z systemu klasy SIEM, zgłoszeń przekazywanych przez użytkowników na dedykowany adres e-mail, zgłoszeń przypisanych w systemie typu helpdesk do odpowiedniej grupy, przez co najmniej system RTIR (Request Tracker Incident Response) lub Jira. Ponadto rozwiązanie musi umożliwiać automatyczne zamykanie obsłużonego zgłoszenia w systemie typu helpdesk, przynajmniej dla rozwiązania RTIR (Request Tracker Incident Response) lub Jira.	
4.	Oprogramowanie musi umożliwiać ręczne utworzenie incydentu.	
5.	Oprogramowanie musi posiadać możliwość automatycznej oraz ręcznej klasyfikacji incydentów ze względu na ich krytyczność.	
6.	Oprogramowanie musi umożliwiać tworzenie własnych definicji klasyfikacji incydentów i ich krytyczności. W ramach wdrożenia Wykonawca wraz z zamawiającym ustali oraz zaimplementuje właściwą klasyfikację incydentów w systemie.	

7.	Oprogramowanie musi umożliwiać śledzenie czasu oraz podjętych działań w ramach utworzonego incydentu oraz raportowanie czasów: Time-to-detect oraz czasów: Time-to-mitigate.	
8.	Oprogramowanie musi umożliwiać łączenie utworzonych incydentów, w tym inteligentne łączenie automatyczne.	
9.	Oprogramowanie musi umożliwiać automatyczne przydzielanie predefiniowanych zadań dla danych typów incydentów.	
10.	Oprogramowanie musi umożliwiać tworzenie i edytowanie procedur reagowania na incydenty w postaci graficznej. System musi umożliwiać stosowanie podstawowych operatorów logicznych i matematycznych przy definicji procedur.	
11.	Oprogramowanie musi umożliwiać automatyczne oraz ręczne przydzielanie incydentów wymagających obsłużenia do pracowników obsługujących system.	
12.	Oprogramowanie musi umożliwiać automatyczną oraz ręczną weryfikację w wewnętrznych oraz zewnętrznych źródłach informacji, charakterystycznych dla danego incydentów atrybutów.	
13.	Oprogramowanie musi umożliwiać zaprojektowanie oraz wdrożenie automatycznych działań reagowania na dane typy incydentów.	
14.	Oprogramowanie musi umożliwiać edycję kodu źródłowego automatycznych działań reagowania. Wymaga się stosowanie języka skryptowego uznanego za powszechny, w jego najnowszej wersji. Np. Python3.	
15.	Oprogramowanie musi umożliwiać tworzenie zbiorczych raportów z utworzonych oraz obsłużonych incydentów.	
16.	Oprogramowanie musi integrować się przynajmniej z następującymi systemami Zamawiającego:	
	- Office 365 / Microsoft Exchange (pobranie lub wysłanie maili),	
	- Slack (wysyłka komunikatów),	
	- Energy Logserver.	
17.	Oprogramowanie musi umożliwiać łatwą integrację z pozostałymi systemami klasy threat intel/threat hunting/threat share za pomocą API.	
18.	System musi posiadać możliwość generowania dashboardów security z danych znajdujących się w SOAR, między innymi statystyk, w tym system musi posiadać możliwość tworzenia i konfiguracji widoków głównych na główny ekran dyspozycyjny w pomieszczeniu SOC.	
19.	Umożliwiać dwustronną komunikację z użytkownikami systemu (np. w celu zebrania dodatkowych informacji od osób związanych z incydentem) oraz operatorami systemu SOAR, na przykład poprzez zastosowanie interaktywnych formularzy.	

20.	Zapewniać zestaw co najmniej 250 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.	
21.	Automatyzować proces analizy otrzymanych danych, realizować funkcje informacyjne, jak również podejmować funkcje naprawcze (np. automatyczna analiza pliku w chmurze sandbox wybranego producenta, wysłanie wiadomości e-mail do użytkownika zainfekowanej stacji końcowej, aby nie otwierał załącznika i blokada na urządzeniu sieciowym dostępu do wskazanych usług dla wybranego użytkownika).	
22.	Posiadać wbudowaną bibliotekę minimum 5 typów incydentów, a także powinno dostarczać specjalizowane typy incydentów związane z integrowanymi systemami, pozwalając jednocześnie na ich edycję lub kopiowanie celem stworzenia własnej karty incydentu.	
23.	Umożliwić wykorzystanie w skryptach własnych bibliotek zewnętrznych oraz programów (np. poprzez umożliwienie uruchomienia skryptów we własnym kontenerze, zawierającym pożądane oprogramowanie).	
24.	Zapewniać możliwość wglądu w kod integracji oraz jego klonowanie pod kątem wprowadzania modyfikacji lub napisania własnej wersji integracji.	
25.	Pozwalać na kopiowanie oraz edycję już istniejących scenariuszy jak również dodawanie nowych.	
26.	Pozwalać na edycję i dodawanie nowych scenariuszy obsługi incydentu (tzw. playbook) za pomocą graficznego interfejsu użytkownika bez konieczności wykorzystania języków skryptowych lub znajomości języków programowania.	
27.	Pozwalać na tworzenie scenariuszy zagnieżdżonych, tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane na zasadzie pod-scenariuszy. Edycja/zmiana pod-scenariusza wpływa automatycznie na wszystkie scenariusze, które go wykorzystują, co ułatwia administrację.	
28.	Pozwalać na tworzenie scenariuszy zawierających:	
	- zadania ręczne,	
	- zadania zautomatyzowane,	
	- zadania warunkowe automatyczne,	
	- zadania warunkowe ręczne,	
	- akwizycję danych przy użyciu formularzy,	
	- filtry danych,	
	- pod-scenariusze.	
29.	Pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy.	
30.	Pozwalać na automatyczne dokumentowanie uruchomionych scenariuszy wraz z wynikami jego działania.	

31.	Umożliwiać wizualizacje przebiegu wykonania scenariusza (wizualizacje rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.).	
32.	Pozwalać na sterowanie wykonaniem scenariusza przez operatora (zadania warunkowe ręczne) drogą korespondencyjną (m.in. z poziomu wiadomości email oraz wiadomości w komunikatorze takim jak np. Microsoft Teams, Slack, Mattermost itp.).	
33.	Pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów.	
34.	Pozwalać na ponowne uruchomienie scenariusza na konkretnym incydencie, jeżeli zajdzie taka potrzeba.	
35.	Pozwalać na zatrzymanie scenariusza w trakcie jego wykonania.	
36.	Pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń).	
37.	Pozwalać na proste monitorowanie stanu wykonania scenariuszy powiązanych z incydentami. Ponadto, w przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza, osoby odpowiedzialne za incydent powinny zostać natychmiast o tym poinformowane.	
38.	Pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.	
39.	Pozwalać na przekazywanie parametrów pomiędzy zadaniami pojedynczego scenariusza.	
40.	Pozwalać na odczytywanie wyników analizy i wykorzystaniu ich w kolejnych zadaniach uruchomionego scenariusza.	
41.	Pozwalać na sprawdzenie historycznych danych na temat uruchomionych scenariuszy/zadań.	
42.	Pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i wedle harmonogramu.	
43.	Pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.	
44.	Pozwalać na tworzenie własnych:	
	- typów incydentów,	
	- pól/etykiet incydentów,	
	- typów wskaźników (ang. indicator),	
	- pól/etykiet wskaźników (ang. indicator),	
	- raportów,	
	- dashboardów.	

45.	Pozwalać na automatyczne wypełnianie pól incydentu bazując na typie incydentu lub jego atrybutach.	
46.	Pozwalać na delegowanie zadań innym członkom zespołu SOC w ramach oceny danego incydentu.	
47.	Pozwalać na współpracę pomiędzy członkami zespołu SOC (np. rozmowa między członkami zespołu a temat incydentu).	
48.	Pozwalać na zapisywanie historycznych incydentów wraz z pełną informacją na temat podjętych akcji obsługi/rozwiązania w celu szkolenia/transferu wiedzy pomiędzy członkami zespołu SOC (Na historię incydentu składają się wyniki działania automatycznych i ręcznych zadań określonych w playbooku, komentarze analityków pracujących nad incydentem, indykatory zagrożenia IOC (IP, URL, domeny, itd.) wyciągane automatycznie i wskazywane ręcznie w czasie obsługi incydentu, elementy analizy oznaczone przez analityków jako dowód w sprawie (np. zrzuty ekranu z widokiem podejrzanych stron web), pliki dodawane do historii obsługi incydentu przez analityków, itp.).	
49.	Pozwalać na export wskaźników kompromitacji do serwerów MISP.	
50.	Pozwalać na import zdarzeń z serwerów MISP.	
51.	Pozwalać na eksport incydentów w formatach STIX 1/2, CSV, PDF.	
52.	Pozwalać na tworzenie wielu instancji integracji tego samego typu do rozwiązań firm trzecich (przykładowo dwie integracje z serwerami IMAP lub zaczytujące dane threat intel z dwóch źródeł w formacie JSON).	
53.	Pozwalać na rozszerzenie możliwości systemu w zakresie tworzenia i edycji scenariuszy poprzez dodanie własnych skryptów realizujących niestandardową logikę operacji warunkowych, filtracji danych, modyfikacji danych, a także skryptów realizujących niestandardową prezentację danych w dashboardach, zadania wykonywane po zakończeniu obsługi incydentu itp.	
54.	Pozwalać na proste wprowadzenie globalnych zestawów poświadczeń w celu ułatwienia użycia wspólnego konta technicznego w wielu integracjach z systemami trzecimi.	
55.	Posiadać zestaw przygotowanych raportów takich jak:	
	- raport na temat incydentów: dzienny, 7- i 30-dniowy,	
	- raport na temat średniego czasu rozwiązania incydentu.	
56.	Pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację pożądanych danych (np. wykres kołowy, słupkowy, liniowy, tabela itp.).	
57.	Pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego	

	języka zapytań) oraz podobieństwa do innych incydentów (related incidents).	
58.	Pozwalać na wizualizację zależności pomiędzy podobnymi incydentami na poziomie wystąpień identycznych indykatorów.	
59.	Pozwalać na eksport raportów w formacie, co najmniej PDF.	
60.	Mieć możliwość działania jako platforma SOAR dla wielu instytucji/klientów z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant).	
61.	Posiadać repozytorium wskaźników (ang. indicators), które kolekcjonuje i koreluje wskaźniki w ramach wszystkich incydentów, alertów i feedów dostarczanych do rozwiązania.	
62.	Posiadać możliwość wykonywania scenariuszy na podstawie zestawu wskaźników (ang. indicators) określonych przez użytkownika.	
63.	Być w stanie obsługiwać formaty strukturalne, takie jak JSON, CSV, STIX 1.X i STIX 2.X itp. w ramach integracji ze źródłami wskaźników (ang. indicators).	
64.	Wspierać minimum następujące typy wskaźników (ang. indicators):	
	- numery kart płatniczych,	
	- IBAN,	
	- adres email,	
	- konto użytkownika,	
	- wyniki CVE,	
	- domena,	
	- FQDN,	
	- nazwy hosta,	
	- IP (v4 oraz v6),	
	- klucz i ścieżka rejestru,	
	- URL,	
	- CIDR.	
65.	Umożliwiać własną definicję wskaźników, jego pól oraz skryptów reputacyjnych.	
66.	Zapewniać użytkownikom możliwość automatycznej weryfikacji wskaźników (tzw. enrichment), wykonując odpowiedni scenariusz lub uruchamiając sprawdzanie na podstawie typu wskaźnika (ang. indicator).	
67.	System musi posiadać natywną integrację z MITRE ATT&CK i przypisywać do incydentów odpowiednie techniki i taktyki.	
68.	System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 1 roku.	

	Szkolenia	Oferowane parametry techniczne/funkcjonalności. Proszę wpisać Spełnia/Nie spełnia/, a jeśli nie spełnia podać jakie inne oferuje
1.	Wykonawca dostarczy voucher szkoleniowy dla 2-óch słuchaczy zarówno dla systemu SIEM/SOAR minimum 4 dni.	
2.	Szkolenie odbędzie się w formie zdalnej.	
3.	Szkolenie musi być prowadzone w języku polskim.	
4.	Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.	
5.	Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.	

	Wdrożenie	Oferowane parametry techniczne/funkcjonalności. Proszę wpisać Spełnia/Nie spełnia/, a jeśli nie spełnia podać jakie inne oferuje
1.	Wykonawcą wdrożenia powinien być przeszkolony zespół producenta.	
2.	Opracowanie harmonogramu wdrożenia systemu SIEM/SOAR.	
3.	Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia.	
4.	Przeprowadzenie instalacji i konfiguracji systemu SIEM/SOAR.	
5.	Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych.	
6.	Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.	
7.	Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.	
8.	Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.	

9.	Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.	
10.	Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.	
11.	Po podpisaniu protokołu odbioru końcowego Wykonawca zapewni dodatkowe wsparcie w wymiarze 64 godzin roboczych rocznie do wykorzystania na prace rozwojowe.	

Signature Not Verified
Dokument podpisany przez Dariusz Zuba
Data: 2026.11.13 18:01:30 CET