Załącznik nr 1

Opis wymagań dotyczący realizacji usługi Security Operations Center w zakresie cyberbezpieczeństwa wraz z oprogramowaniem w modelu usługowym

1 Wymagania na usługę Centrum Monitorowania Bezpieczeństwa (SOC)

1.1 Monitoring

1.1.1 W ramach monitoringu Oferent zobowiązuje się do świadczenia usługi I Linii SOC przez wszystkie dni w roku 24 godziny na dobę w zakresie:

a. bieżącego monitorowania zdarzeń i incydentów pojawiających się w systemie SIEM Zamawiającego,
b. wstępnej analizy incydentów zgodnie z ustalonymi procedurami i scenariuszami,
c. analizy incydentów pod względem wystąpienia tzw. false-positive,
d. zebranie i usystematyzowanie materiału dotyczącego incydentu,
e. ustalenie poziomu incydentu (triage),
f. wystawianie zgłoszenia w systemie obsługi zgłoszeń oraz informowanie dodatkowym kanałem informacji w przypadku wystąpienia krytycznych incydentów,
g. samodzielnej obsługi incydentów o niskim priorytecie.

2. Zapewnić czas reakcji na zdarzenia wynikające z ustalonych reguł korelacyjnych na poziomie 60 min
3. Realizować wsparcia w optymalizacji i parametryzację reguł SIEM w oparciu o pozyskane informacje o zagrożeniach.
4. Realizować okresowe (miesięczne) raportowanie dot. realizacji usługi.

1.2 Zarządzanie Incydentami:

1.2.1 Wykonawca będzie realizował usługę Zarządzania Incydentami przez wszystkie dni w roku 24 godziny na dobę w zakresie:

a) Reakcji na incydent.
b) Analizy wykrytych incydentów.

1.2.2 Oferent zapewni Czas reakcji analityków na incydent, rozumiany jako czas od momentu powzięcie przez Operatorów I linii SOC decyzji o konieczności przekazania obsługi Incydentu Bezpieczeństwa do II linii do momentu faktycznego podjęcie obsługi incydentu przez Analityka II linii:

a) w godzinach roboczych: 60 min
b) poza godzinami roboczymi: 60 min

1.2.3 Analizę pozostałych logów pod kątem:

a) wykrycia anomalii, które nie wpadły w monitorowane reguły korelacyjne,
b) proponowania nowych reguł korelacyjnych poszerzających obszar monitorowania przez I linię SOC.

1.2.4 Optymalizację uruchomionych reguł korelacyjnych, w tym występujących False Positive.

1.2.5 Proponowanie nowych rozwiązań bezpieczeństwa, systemów, usług w celu powiększania obszaru bezpieczeństwa Zamawiającego.

1.2.6 Okresowe raportowanie dot. występujących incydentów w infrastrukturze klienta, trendów, pojawiających się zagrożeń w Internecie.

2 W ramach usługi SOC zapewnione będzie:

2.1 Skanowanie podatności infrastruktury wg ustalonego harmonogramu (nie rzadziej niż 4 razy do roku) zakończone raportem wskazującym działania dla usunięcia wykrytych podatności

2.2 Specjalistyczne wsparcie inżynierskie w wyprowadzaniu incydentu - minimum do 6 godzin miesięcznie (w tym nie więcej niż 3 godziny on-site)

2.3 Specjalistyczne wsparcie w remediacji wykrytych podatności – minimum 3 godziny kwartalnie

2.4 Wykonanie przedwdrożeniowego audytu polityk bezpieczeństwa zakończonego raportem.

3 Wymagania do systemu SIEM

3.1 Rozwiązanie SIEM musi zapewniać skalowalną architekturę spełniającą następujące wymagania:

a. wszystkie urządzenia odpowiedzialne za zbieranie informacji (kolektory), mogą być dostarczone tylko w postaci rozwiązań wirtualnych lub platformach sprzętowych pochodzących od tego samego producenta
b. kolektory muszą mieć możliwość buforowania otrzymanych informacji. System musi mieć możliwość definiowania rozmiaru tego bufora oraz monitorowania jego zajętości
c. system SIEM musi mieć możliwość ograniczenia ilości zdarzeń przesyłanych ze źródeł do poszczególnych kolektorów
d. dane przesyłane do systemu SIEM muszą podlegać kompresji na poziomie odbierania ich przez kolektory
e. komunikacja pomiędzy modułami wchodzącymi w skład systemu SIEM, musi odbywać się z wykorzystaniem szyfrowanego protokołu HTTPS.
f. z poziomu warstwy zarządzającej, kolektory mają mieć możliwość aktualizacji wersji swojego oprogramowania
g. rozwiązanie SIEM ma posiadać możliwość aktualizacji online dla parserów, reguł, raportów oraz typów wspieranych urządzeń, niezależnej od oprogramowania systemowego (OS)

3.2 Warstwa przechowywania i korelacji danych ma spełniać następujące wymagania:

h. implementacja ma być zrealizowana w oparciu o rozwiązania wirtualne lub platformy sprzętowe pochodzące od tego samego producenta

i. rozwiązanie ma wspierać nie mniej niż poniżej wymienione środowiska wirtualizacyjne:
    i. VMWare
    ii. Hyper-V
    iii. KVM
    iv. AWS
    v. Azure
j. system SIEM musi mieć możliwość skalowania wertykalnego oraz horyzontalnego poprzez dodawanie kolejnych analogicznych modułów lub rozbudowę podzespołów maszyn wirtualnych. W przypadku środowiska wirtualnego, zwiększenie parametrów maszyn lub dodanie nowych modułów, nie może wpływać na koszty licencji produktu
k. system SIEM musi być wolny od wszelkich ograniczeń licencyjnych dotyczących liczby lub wielkości zdarzeń i danych, które przechowuje. Jedyną dopuszczalną barierą w kontekście przechowywanych danych może być pojemność dysku twardego.
l. system SIEM 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.)
m. system SIEM powinien być zdolny do przechowywania zgromadzonych danych zarówno w ich oryginalnej, nieprzetworzonej formie (logi zdarzeń surowych) jak i w formie danych przetworzonych (logi zdarzeń sparsowanych/danych znormalizowanych)
n. zebrane dane muszą być przechowywane w sposób skompresowany
o. system musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adresy email, nazwy użytkowników.
p. system SIEM nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, nie mniej niż: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami
q. klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, zdarzeń i innych ustrukturyzowanych informacji
r. maszyny wirtualne systemu SIEM mają działać w oparciu o system Unix/Linux lub Windows, który ma mieć możliwość aktualizacji. Aktualizacje zarówno rozwiązania SIEM jak i bazowego systemu operacyjnego muszą być dostarczane przez producenta rozwiązania w wygodnej formie pliku aktualizacyjnego

3.3 Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez aktywne wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich metod pobierania zdarzeń jak:

a. SNMP
b. Syslog
c. Windows Management Instrumentation (WMI) i Open Management Infrastructure (OMI)
d. Microsoft RPC
e. JDBC lub ODBC
f. VM SDK
g. JMX
h. Telnet
i. SSH
j. NetFlow
k. HTTPS
l. IMAP
m. IMAP over SSL
n. POP3
o. import z pliku CSV
p. REST API

3.4 Wymaga się, aby kolektory danych systemu SIEM umożliwiały eliminację danych uznanych za nieistotne lub zbędne. Ta funkcjonalność nie powinna wpływać na sposób licencjonowania systemu

3.5 Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

3.6 Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

3.7 Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

3.8 System SIEM musi być w stanie obsłużyć minimum **5000** EPS (events per secons) oraz umożliwiać monitorowanie pod kątem bezpieczeństwa 1000 zasobów IT, w tym kluczowych stacji roboczych i serwerów.

3.9 Rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu aplikacje typu agent lub z wykorzystaniem natywnego narzędzia rsyslog

3.10 Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:

a. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows
b. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application

c. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS
d. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu
e. agent Windows musi mieć możliwość buforowania zbieranych zdarzeń w wypadku utraty komunikacji z pozostałymi elementami klastra SIEM.

3.11 System SIEM musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis). Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

3.12 System musi posiadać co najmniej 500 gotowych reguł korelacyjnych wprowadzonych przez producenta.

3.13 Aktualizacja reguł korelacyjnych przygotowywanych przez producenta musi być wykonywana gotowym i wygodnym mechanizmem w interfejsie graficznym. Obowiązkowe jest oddzielenie tego typu aktualizacji od aktualizacji systemu

3.14 System SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

3.15 System SIEM musi być w stanie wykryć usługi Active Directory oraz LDAP oraz wyświetlać informacje o strukturze katalogowej drzewa w GUI

3.16 Musi istnieć możliwość wykorzystania struktury katalogowej drzewa LDAP jako warunku podczas tworzenia raportów i w ramach pozostałych mechanizmów analitycznych

3.17 Muszą być wspierane zewnętrzne metody uwierzytelniania użytkowników SIEM, nie mniej niż:
a. Active Directory lub LDAP
b. RADIUS
c. SAML

3.18 Musi istnieć integracja z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI):
a. wsparcie dla plików CSV musi być wykonywalne z wykorzystaniem interfejsu graficznego GUI
b. definicje w ramach integracji muszą zawierać nie mniej niż:
i. adresy IP
ii. domeny
iii. sumy kontrolne (hash)
iv. adresy URL
c. wymagane jest, aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 50 tysięcy wpisów
d. wraz z systemem SIEM musi być wspierany, już zintegrowany, zestaw baz zagrożeń niekomercyjnych (open source)
e. system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym.

f. system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi
g. system musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal, w tym również pochodzących od producenta samego systemu SIEM
h. system musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla wbudowanych reguł. Reguły dostarczone przez producenta muszą być skatalogowane według wspomnianej nomenklatury jak również skatalogowane muszą być generowane przez nie alarmy. Ilość reguł wskazujących na taktyki MITRE ma wynosić nie mniej niż 300.

3.19 System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML

3.20 Dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji:

a. Bar
b. Pie
c. Line
d. Table
e. Combination (line and table view)
f. Treemap
g. Single values
h. Gauges
i. Geographical Map

3.21 Notyfikacje oraz zarządzanie incydentami, system SIEM musi:

a. posiadać narzędzia pozwalające na samodzielne tworzenie polityk informujących o incydentach
b. posiadać możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty
c. możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty musi być możliwa w oparciu o role z podziałem na użytkowników mających pełne prawa do uruchamiania skryptów i na użytkowników zgłaszających żądanie uruchomienia skryptu, które to żądanie musi być zatwierdzone przez użytkownika nadrzędnego
d. posiadać możliwość integracji w oparciu o API z zewnętrznymi systemami do obsługi zgłoszeń (ticketing systems) takimi jak ServiceNow, ConnectWise oraz Remedy
e. mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system)
f. mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów

3.22 Analityka.

System SIEM musi mieć możliwość:

a. wyszukiwania zdarzeń (events) w trybie bieżącym oraz historycznym
b. wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych

c. wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne.
d. wyszukiwania w oparciu o niemniej niż następujące operatory: include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex
e. wykorzystania mechanizmów Machine Learning w oparciu o zgromadzone zdarzenia
f. tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną
g. możliwości eksportowania raportów do formatów CSV, PDF
h. wyszukiwania zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego
i. wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej
j. automatycznego korelowania użytkownika z jego lokalizacją i adresem IP:
    v. musi istnieć możliwość wzbogacania zdarzeń (events) przy których dane użytkownika pozbawione są informacji o adresie IP
    vi. wykorzystanie funkcjonalności lokalizacji adresu IP (Geo IP) w oparciu o bazę pochodzącą od tego samego producenta
    vii. Musi istnieć możliwość łączenia różnych kont takich jak login w active directory, adres e-mail, nazwa konta w usługach chmurowych dla jednego użytkownika w ramach funkcji tzw. aliasu.

3.23 Powinna istnieć możliwość wykorzystania zewnętrznych silników sztucznej inteligencji, np. OpenAI/ChatGPT-4 lub odpowiednika do prowadzenia dialogu operatora z systemem.

3.24 Dla danych przechowywanych na dysku lokalnym lub udziale NFS system SIEM musi pozwalać na realizowane w oparciu o polityki archiwizowanie danych do innego udziału, takiego jak np. NFS

3.25 Integralność danych zapisywanych na dysku lokalnym lub udziale NFS związanych ze zdarzeniami musi być weryfikowalna z wykorzystaniem GUI w oparciu o przeliczenie sum kontrolnych, które obliczane były w momencie zapisywania danych o zdarzeniach na dysk systemu SIEM.

3.26 Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

a. kolektor parsujący;
b. kolektor logów;
c. kolektor korelacyjny;
d. kolektor zdarzeń;
e. kolektor sztucznej inteligencji;
f. kolektor reakcyjny;
g. kolektor kontrolujący.

3.27 Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

3.28 Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś. zdarzeń na sekundę (EPS) w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

3.29 Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

3.30 Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

3.31 Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska, obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

3.32 Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

3.33 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.

3.34 Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

3.35 Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

3.36 Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.

3.37 Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

3.38 Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tyś zdarzeń na sekundę (EPS). Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

3.39 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.)

3.40 Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

3.41 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.

3.42 Producent oferowanego systemu musi utrzymywać publicznie dostępną dokumentację.

3.43 Producent oferowanego systemu musi wspierać integrację z przynajmniej jednym rozwiązaniem typu SOAR, gdzie możliwe musi być co najmniej:

a. uruchamianie procedur wykonawczych SOAR (tzw. Playbook) z poziomu SIEM

b. wykonywanie operacji na systemach zintegrowanych z SOAR, np. pobranie listy zablokowanych adresów IP na firewall, dodanie do blokady adresu URL, zweryfikowanie reputacji IOC w serwisie internetowym.

3.44 Dla systemu SIEM muszą być dostępne certyfikowane szkolenia w tym poprzez portal producenta.

3.45 Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów. Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.

3.46 W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących 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.

3.47 System ma gwarantować możliwość elastycznej, bezkosztowej rozbudowy o kolejne źródła logów.

3.48 Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

3.49 W ramach systemu SIEM Oferent zobowiązuje się do zapewnienia licencji dla maksymalnie 200 obiektów będących źródłem powstania logów, określonych na etapie wdrożenia.

4 Wymagania dla usługi EDR

Zamawiający dysponuje systemem klasy EDR ESET na 350 stanowisk.

Zamawiający wymaga zintegrowania posiadanego systemu EDR z oferowanym systemem SOAR

5 Wymagania do systemu SOAR

Oferent zobowiązany jest posiadać w swoim centrum operacyjnym system klasy SOAR umożliwiający automatyzację obsługi i analizy incydentów Zamawiającego
System SOAR musi spełnić poniższe wymagania

5.1 musi być zainstalowany w licencji multi-tenant z separacją danych dla poszczególnych tenantów (klientów).

5.2 musi posiadać elastyczną możliwość integracji z systemami Zamawiającego, 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 wtyczek/konektorów.

5.3 musi mieć możliwość definiowania SLA na poziomie obsługiwanych incydentów

5.4 musi posiadać możliwość integracji z dostarczonym systemem SIEM, EDR, XDR w zakresie przekazywania informacji o incydentach oraz natywnie wspierać integrację z urządzeniami użytkowanych przez Zamawiającego.

5.5 musi posiadać logi audytowe, które dostarczą informacji o aktywności w systemie SOAR, włączając informacje o uruchomionych playbookach na poszczególnych urządzeniach Zamawiającego. Informacje zawarte w tych logach, powinny zawierać dane kto i kiedy uruchomił dany playbook oraz jakie akcje zostały wykonane w ramach tego playbooka.

5.6 musi mieć możliwość definiowania cyklicznego generowania raportów z obsłużonych incydentów.

5.7 Wbudowane funkcje współpracy, takie jak War Room dla każdego incydentu, ścisła integracja z narzędziami do zarządzania sprawami/ ticketami,

5.8 musi umożliwiać zdalne uruchamianie Playbook-ów i kolekcję danych z infrastruktury Zamawiającego za pośrednictwem agenta lub agentów systemu SOAR, zainstalowanych w tejże infrastrukturze.

5.9 Możliwość limitowania ilości pobieranych incydentów z systemów klienckich tj: SIEM, EDR etc.

5.10 Rozwiązanie musi umożliwiać tworzenie własnych mappingów w zależności od źródła i typu incydentu.

5.11 Musi posiadać szeroki zakres możliwych konfiguracji, minimum 150 wspieranych wtyczek/konektorów, możliwość ich modyfikacji lub napisanie własnych wtyczek (w języku python, dopuszcza się narzędzie powershell).

5.12 Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz oferować nieograniczone możliwości w zakresie ilości dostępnych scenariuszy, które nie mogą wpływać na poziom licencjonowania.

5.13 Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: mechanizmy reakcji, scenariusze reakcji. Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: The Hive, itp. lub został stworzony przez modyfikację oprogramowania otwartego.

6 Wymagania na wdrożenie usługi:

6.1 Zamawiający nie dopuszcza świadczenia usługi monitoringu i zarządzania incydentami na rozwiązaniu typu open source.

6.2 System SIEM i SOAR musi natywnie wspierać urządzenia sieciowe znajdujące się w infrastrukturze Zamawiającego.

6.3 Kwalifikacje oraz wielkość zespołu wdrożeniowego:

6.3.1 Oferent dysponuje zespołem inżynierów/wdrożeniowców na potrzeby specjalistycznego wsparcia inżynierskiego w wyprowadzaniu incydentu – minimum do 6 godzin miesięcznie (w tym nie więcej 3 godziny on-site)

6.3.2 Oferent dysponuje co najmniej 2 osobami posiadającymi certyfikat Blue Team min. Level 1

6.3.3 Oferent dysponuje co najmniej 2 osobami posiadającymi certyfikat audytora wiodącego ISO 27001 (lub równoważny)

6.3.4 Oferent dysponuje co najmniej 2 osobami posiadającymi certyfikat audytora wewnętrznego systemu zarządzania ciągłością działania wg PN-EN ISO 22301

6.3.5 Oferent dysponuje co najmniej 2 osobami posiadającymi certyfikat potwierdzający kompetencje w obsłudze i utrzymaniu systemu SIEM i SOAR

6.3.6 Oferent dysponuje co najmniej 2 specjalistami z zakresu rozwiązań sieciowych, rozwiązań macierzowych, rozwiązań kopii zapasowych, wizualizacji oraz rozwiązań klasy EDR

6.3.7 Oferent dysponuje min. 6 osobami (zatrudnionymi na podstawie umowy o pracę) skierowanymi przez Wykonawcę do realizacji zamówienia posiadającymi kwalifikacje zawodowe których mowa w par. 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

6.3.8 Oferent potwierdzi doświadczenie i kompetencje wskazanych wyżej osób odpowiednimi certyfikatami. Zamawiający dopuszcza możliwość łączenia specjalności z poszczególnych zakresów.

6.4 Wykonawca zobowiązany jest do Przygotowania zestawu zadań wymaganych do uruchomienia usługi Centrum Monitorowania Bezpieczeństwa:

a) Harmonogram wdrożenia usługi Security Operation Center;
b) Przygotowania i wdrożenia do 10 scenariuszy użycia/reguł korelacyjnych dla zidentyfikowanych podczas analizy przedwdrożeniowej
c) Przygotowania i wdrożenia do 5 scenariuszy reagowania (Playbooków) na incydenty bezpieczeństwa wykryte na podstawie zaproponowanych scenariuszy użycia/reguł korelacyjnych.