# **Szczegółowy opis przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa **Systemu** składającego się z:

1. rozwiązania służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management) zwanego dalej **Systemem SIEM**

oraz

1. rozwiązania służącego do automatyzacji i strukturyzacji procesów w systemach informatycznych (system klasy SOAR - Security Orchestration, Automation And Response) zwanego dalej **Systemem SOAR,**

wraz ze:

- wsparciem technicznym i Gwarancją na okres 36 miesięcy oraz

- **Usługami Wykonawcy** w maksymalnej łącznej ilości **3 500** **godzin** zegarowych do wykorzystania w całym okresie obowiązywania Umowy, obejmującymi Usługi Instalacyjno-Wdrożeniowe, Usługi Szkoleniowe oraz Usługi Wsparcia Eksperckiego Wykonawcy oraz

- **Usługami Szkoleniowymi Producenta** w maksymalnej łącznej liczbie **232 szkolenia** do wykorzystania w całym okresie obowiązywania Umowy

Zamawiający przewiduje możliwość wdrożenia Systemu w różnych lokalizacjach, konfiguracjach i różnym czasie w trakcie obowiązywania Umowy, zgodnie ze złożonymi przez Jednostki wnioskami o zamówienie Zamawiający wymaga aby wdrożenie Systemu było możliwe jako niezależne instancje i bez ograniczenia co do ilości tych instancji. Przy czym Zamawiający wymaga aby korzystanie z Systemu było możliwe w co najmniej dwóch niezależnych grupach licencyjnych tj. jedna grupa dla Ministerstwa Sprawiedliwości, z możliwością korzystania z Systemu przez jednostki sądownictwa w ramach tej samej grupy licencji z możliwością dowolnego przenoszenia/współdzielenia licencji pomiędzy instancjami w ramach tej samej grupy (licencje przenaszalne), i drugiej analogicznej grupy dla Centralnego Zarządu Służby Więziennej.

# Wymagania ogólne

1. System SIEM musi być dojrzałym, uznanym na rynku produktem – jako potwierdzenie spełnienia wymagania uznane będzie:
   1. zakwalifikowanie oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert)

lub

* 1. zakwalifikowanie oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert).

1. Nie dopuszcza się rozwiązań open source.
2. System SIEM musi być w sprzedaży na rynku co najmniej 3 lata oraz posiadać wsparcie techniczne Producenta w języku polskim.
3. System SIEM musi umożliwiać wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie:
   1. monitorowania infrastruktury
   2. monitorowanie dostępności usług
   3. wydajności aplikacji.
4. System SIEM musi umożliwiać tworzenie własnych, nieprzewidzianych przez Producenta funkcjonalności związanych z analizą danych obejmujących:
   1. mechanizmy pobierania danych,
   2. raporty, dashboardy i formularze,
   3. nowe funkcje analityczne,
   4. nowe sposoby wizualizacji,
   5. mechanizmy powiadamiania.
5. Architektura Systemu SIEM musi umożliwiać rozdzielenie na osobne serwery funkcji:
   1. pobierania danych,
   2. przechowywania, wyszukiwania i zarządzania bazą zebranych logów,
   3. warstwy analitycznej i interfejsu użytkownika,
   4. monitorowania dostępności systemu SIEM oraz zarządzania poszczególnymi komponentami
6. Licencja musi dopuszczać dowolne kształtowanie architektury Systemu SIEM, w szczególności stosowanie dowolnej liczby komponentów poszczególnych funkcji opisanych w punkcie powyżej. Rozbudowa Systemu SIEM o kolejne elementy przetwarzające, analizujące, zbierające nie może się wiązać z żadnymi dodatkowymi kosztami licencyjnymi.
7. Wszystkie dostarczone licencje muszą być przenaszalne tj. pozwalać co najmniej na łączenie, podział lub rozbudowę Systemu oraz dowolne przypisywanie licencji pomiędzy Jednostkami lub w obrębie Jednostek (np. w przypadku zakupu kolejnych licencji) przez cały okres obowiązywania Umowy.
8. Wszystkie komponenty wchodzące w skład Systemu SIEM i Systemu SOAR muszą być w wersji produkcyjnej.
9. System SIEM musi być dostarczony od tego samego Producenta co System SOAR.
10. System SIEM i System SOAR musi zapewniać skalowalność pozwalającą na pracę w dużych organizacjach.
11. System SIEM i System SOAR musi mieć możliwość pracy w architekturze pozwalającej na instalację i konfigurację w wielu lokalizacjach.
12. System SIEM i System SOAR musi wspierać granularne zarządzanie poziomami dostępu oparte o role użytkowników (RBAC).
13. System SIEM musi mieć możliwość uruchomienia w architekturze zapewniającej wysoką dostępność.
14. System SIEM musi posiadać wbudowane mechanizmy kompresji danych przetwarzanych online na zasobach dyskowych na poziomie minimum 30% w stosunku do wielkości otrzymywanych danych.
15. System SIEM i System SOAR muszą być objęte wsparciem technicznym Producenta przez cały okres na jaki zostały kupione licencje. Wsparcie to w szczególności musi pozwalać na nieodpłatne instalowanie wszelkich poprawek, aktualizacji i najnowszych wersji Oprogramowania.
16. Wykonawca dostarczy najnowsze wersje Oprogramowania dla Systemu SIEM i Systemu SOAR na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez Producenta rozwiązania.

# Wymagania funkcjonalne – pozyskiwanie danych

1. System SIEM musi umożliwiać pobieranie logów/zdarzeń co najmniej z następujących systemów i aplikacji:
   1. Systemy Windows 2003/2008/2012/2016/2019/2022 oraz XP/7/8.x/10/11.
   2. Systemy Linux (każda dystrybucja)
   3. Urządzanie sieciowe Cisco, Nortel, Alcatel, MikroTik, Juniper, Fortinet, Dell, Extreme networks
   4. Przez pozyskiwanie logów rozumie się:
      1. pobranie logów i zapisanie w bazie systemu SIEM,
      2. klasyfikacja zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.)
   5. normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source\_ip itp.
2. System SIEM musi umożliwiać pobieranie logów co najmniej następującymi protokołami:
   1. syslog UDP/TCP
   2. logi i informacje przechowywane w bazach danych. Nie mniej niż Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie). System musi pozwalać na wywołanie dowolnego zapytania do bazy danych w celu pobrania odpowiednich logów (nie tylko tabele audytowe).
   3. pliki tekstowe,
   4. logi JMS, JMX,
   5. dane z systemów wirtualizacji,
   6. dane z systemów chmurowych,
   7. NetFlow v5 i v9, sFlow, jFlow, IPFIX,
   8. zbiory wskazane w katalogach

Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

1. System SIEM musi pozwalać na modyfikację mechanizmów klasyfikacji zdarzeń i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania nie mogą nadpisywać ww. modyfikacji.
2. System SIEM musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń do warstwy 4 ISO/OSI oraz do warstwy 7, dla następujących protokołów:
   1. DHCP,
   2. DNS,
   3. HTTP,
   4. IMAP,
   5. SIP,
   6. SMB,
   7. SMTP.
3. Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze.
4. Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http\_user\_agent) oraz opcjonalnie agregację danych.
5. Musi istnieć możliwość przyjmowania przez system SIEM danych w postaci strumienia TCP i automatycznego parsowania na zdarzenia.
6. System SIEM musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w strefach DMZ lub lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie.
7. Agent musi zapewniać możliwość szyfrowania i uwierzytelnia komunikacji z serwerem centralnym.
8. Musi istnieć możliwość ograniczenia przepustowości wykorzystywanej przez agenta do transmisji danych.
9. Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie
10. Konfiguracja i zarządzanie agentami, po podłączeniu do systemu SIEM musi odbywać się centralnie.
11. Rozwiązanie musi zapewnić możliwość grupowania monitorowanych systemów poprzez agentów.
12. Rozwiązanie powinno zapewniać dostępność agentów, udostępnionych przez Producenta rozwiązania, do zbierania zdarzeń z serwerów z systemami operacyjnymi Microsoft Windows, Unix/Linux, lub innych serwerów aplikacyjnych, bez konieczności wnoszenia dodatkowych opłat lub zawierać odpowiedni pakiet licencji, gwarantujący możliwość zainstalowania stosownego agenta na każdym z potencjalnych źródeł, które Jednostki będą chciały podłączyć do Systemu SIEM.
13. System SIEM musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych.
14. Oprócz źródeł wymienionych wyżej System SIEM musi umożliwiać pobieranie informacji z wykorzystaniem poniższych mechanizmów:
    1. dane wydajnościowe Windows Performance Monitor,
    2. dowolne dane WMI,
    3. wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym,
    4. Zmiany w zawartości plików i kluczy rejestrów.
    5. Pliki tekstowe na zdalnych serwerach poprzez SSH, CIFS i NFS.
15. System SIEM musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię.
16. System SIEM musi umożliwiać tworzenie bazy definicji formatów logów.

# Wymagania funkcjonalne – normalizacja danych

1. System SIEM musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.) bez konieczności przeprowadzania ponownego odbudowywania bazy danych lub ponownego zaczytania danych historycznych. System SIEM musi pozwalać na równoległe używanie różnych sposobów normalizacji logów.
2. Poniższe parsery danych muszą być dostępne w systemie SIEM, nie dopuszcza się wytwarzania poniższych parserów na etapie wdrożenia.
   1. System SIEM musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenia parserów. Nazwy pól powinny być określone strukturą XML
   2. System SIEM musi umożliwiać obsługę logów w formacie CEF bez konieczności tworzenia parserów. Nazwy pól powinny być określone strukturą CEF.
   3. System SIEM musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenia parserów. Nazwy pól powinny być określone strukturą JSON.
   4. System SIEM musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenia parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp. ) oraz wartości pól w cudzysłowach.
3. System SIEM musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski” powinno tworzyć pole „user” o wartości „jkowalski”.
4. Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach:
   1. Katalogi LDAP,
   2. Bazy danych,
   3. Bazy noSQL
   4. Hadoop
   5. Dane geolokalizacyjne.
      1. W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie powinny być przechowywane razem z logami, a wzbogacanie powinno odbywać w locie w trakcie odczytu danych z źródeł zewnętrznych.
5. System SIEM musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.
6. System SIEM musi umożliwiać analizę logów w różnych językach, w tym co najmniej w języku angielskim i polskim. Znaki w logach źródłowych kodowane przy użyciu różnych stron kodowych muszą być konwertowane do wspólnego kodowania (preferowane UTF8 lub UTF16).
7. Licencja nie może ograniczać w żaden sposób liczby podłączonych urządzeń (tzn. źródeł danych).
8. System SIEM musi umożliwiać przygotowanie parsera danych w oparciu o GUI. Bez konieczności pisania jakiegokolwiek kodu.
9. System SIEM musi pozwalać na edycję zdefiniowanych parserów danych źródłowych bez konieczności ponownego przygotowywania i zapisania danych historycznych (już istniejących w bazie danych proponowanego rozwiązania) lub przebudowywania bazy danych zawierających zdarzenia.
10. System SIEM posiada możliwość zmiany sposobu normalizacji danych w trakcie jego używania (np. dodanie nowych pól, zmiana znaczenia lub nazwy istniejących itp.) bez konieczności przeprowadzania ponownego odbudowywania bazy danych. System SIEM pozwala na równoległe używanie różnych sposobów normalizacji logów

# Wymagania funkcjonalne – wyszukiwanie i przechowywanie danych

1. System SIEM musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwy w oparciu o te same narzędzia.
2. System SIEM musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów ww. klastra w celu spełnienia wymagań dot. wydajności lub dostępności (zwiększenie liczby kopii danych). Klastry muszą umożliwiać funkcjonowanie w środowiskach złożonych z wielu lokalizacji, przy czym konfiguracja replikacji danych musi pozwalać na określenie, w której lokalizacji dostępne są kopie zebranych informacji.
3. System SIEM musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS lub NFS lub iSCSI w celu przechowywania danych archiwalnych i danych COLD. Dane COLD powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line. Dopuszczalne jest by dane dostępne były z mniejszą wydajnością.
4. Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem.
5. System SIEM musi pozwalać na dowolne przeszukiwanie danych za pomocą języka zapytań. Dodatkowo system w/w klasy powinien umożliwiać zastosowanie funkcji matematycznych/statystycznych podczas operacji na wynikach z wyszukiwania danych.
6. System SIEM samodzielnie zarządza retencją danych. Wymagana jest obsługa co najmniej dwóch etapów życia danych: „bieżące” i „historyczne”. Z każdym etapem związane jest miejsce przechowywania danych. Migracja danych następuje automatycznie po określonym czasie (wiek danych) lub osiągnięciu określonej objętości. Istnieje możliwość stworzenia różnych schematów retencji dla różnych typów danych. Dane historyczne są dostępne w ten sam sposób co dane bieżące, w szczególności nie jest dopuszczalne wymaganie jakichkolwiek czynności związanych z odtwarzaniem danych historycznych

# Wymaganie funkcjonalne – narzędzia analityczne danych

1. Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń, System SIEM musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól.
2. System SIEM musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach, jeśli tylko są dostępne. System musi uwzględniać przy prezentacji wyniku możliwość pozyskiwania logów z urządzeń skonfigurowanych w innych strefach czasowych.
3. System SIEM musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone w wielu formatach – minimum PDF, CSV.
4. Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje:
   1. Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego).
   2. Funkcje wykrywania anomalii danych liczbowych. Rozwiązanie musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego.
   3. Rozwiązanie musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze.
   4. Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól.
   5. Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%).
5. System SIEM musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia czy dnia tygodnia).
6. System SIEM musi pozwalać na akcelerację zapytań i raportów, które wykonywane są często, tak by automatycznie budował agregaty pozwalające na szybkie wykonania raportu obejmującego dowolnie długie okresy czasu. Akceleracja musi być dostępna zarówno dla raportów wbudowanych jak i własnych definiowanych przez użytkownika. Raporty takie powinny być dostępne w czasie nie przekraczającym kilku sekund od ich uruchomienia dla dowolnego okresu czasu.
7. System SIEM musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem:
   1. Tabel,
   2. List zdarzeń,
   3. Wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy),
   4. Map,
   5. Map kolorowanych.
8. Musi istnieć możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na standardowych dashboardach systemu.
9. Musi istnieć możliwość tworzenia interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie jak np. pola tekstowe, listy wyboru, checkbox itp. pozwalające na parametryzacje wyświetlanych informacji. Musi istnieć możliwość tworzenia ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych).
10. Musi istnieć możliwość definiowania akcji typu drill-down powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny obejmować zewnętrzny URL lub raport/dashboard w samym systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pól, których dotyczy akcja drill-down. Musi istnieć możliwość przekazania parametrów metodami GET i POST.
11. Musi istnieć możliwość tworzenia na podstawie tego samego zapytania do bazy systemu zarówno alarmów jak i raportów. Musi istnieć możliwość utworzenia panelu dashboardu na podstawie dowolnego raportu.
12. System SIEM musi umożliwiać konfigurację klastrów wysokiej dostępności z równoważeniem obciążenia (klastry Active/Active). Musi istnieć możliwość konfiguracji dowolnej liczby węzłów klastra. Równoważenie obciążenia pomiędzy komponentami systemu SIEM nie może wymagać stosowania zewnętrznego rozwiązania je rozkładającego (tzw. loadbalancer) oraz nie może wymagać zakupu żadnej dodatkowej licencji.

# Wymagania funkcjonalne – analiza zdarzeń bezpieczeństwa

1. System SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach).
2. System SIEM musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danego systemu SIEM.
3. Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości.
4. System SIEM musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie.
5. Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.).
6. System SIEM musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:
   1. Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych,
   2. Możliwość przypisania incydentu do osoby,
   3. Możliwość zmiany statusu i priorytetu incydentu,
   4. Możliwość tworzenia komentarzy,
   5. Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy.
   6. Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki.
   7. Możliwość raportowania wydajności obsługi incydentów.
7. System SIEM musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu.
8. System SIEM musi umożliwiać wzbogacanie informacji o incydentach poprzez automatyczne uruchomienie dodatkowych zapytań i raportów, które pozwolą na automatyczną ocenę wpływu lub potwierdzenie istnienia incydentu.
9. W systemie SIEM musi istnieć możliwość pracy nad jednym incydentem, przez większą liczbę analityków w tym samym czasie. Każda akcja wykonana przez każdego z analityków musi zostać odnotowana w historii incydentu (do analizy dla przełożonych).
10. System SIEM musi pozwalać na stworzenie dowolnych szablonów sekwencji, które mogą zawierać wiele reguł korelacyjnych w celu szybszej analizy ataku
11. System SIEM musi posiadać wybudowany i w pełni modyfikowalny silnik do oceny punktowej na podstawie ryzyka reguły korelacyjnej (tzw. Risk Score).
12. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto.
13. Musi istnieć możliwość prezentacji opisu zasobu, w postaci serwera lub stacji roboczej, obejmującej: nazwę, istotność, właściciela, funkcję, kontakt do administrator, nawet jeżeli w samym logu występuje wyłączenie adres IP lub MAC tego zasobu. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane.
14. System SIEM musi umożliwiać prezentację zdarzeń związanych z użytkownikiem niezależnie od tego z jakiego konta korzystał. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane.
15. System SIEM musi umożliwiać korzystanie z zewnętrznych subskrypcji tzw. wskaźników kompromitacji (ang. IOC). System musi wspierać dowolne subskrypcje zgodne z protokołami:
    1. http,
    2. ftp,
    3. TAXII,
    4. Threatconnect
    5. System musi również interpretować pliki w formacie CSV, STIX, OpenIOC, tekstowym interpretowanym z wykorzystaniem REGEX.
16. System SIEM musi wspierać ww. wskaźniki wobec pól reprezentujących:
    1. Certyfikat X509,
    2. Adres email,
    3. Nazwa pliku,
    4. Suma kontrolna pliku,
    5. URL,
    6. Adres hosta lub domena,
    7. Adres IP,
    8. Nazwa procesu,
    9. Suma kontrolna procesu,
    10. Klucze rejestru,
    11. Nazwa usługi systemowej,
    12. Nazwa użytkownika,
    13. Musi istnieć możliwość rozbudowy funkcjonalności o nowe typy wskaźników, dokonywanej samodzielnie, przez administratora.
17. Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach.
18. System SIEM musi posiadać predefiniowane raporty raporty/dashboardy związane z zarządzaniem bezpieczeństwem, co najmniej uwzględniające następujące zagadnienia:
    1. istotne zdarzenia bezpieczeństwa uwzględniające istotność zasobu informatycznego,
    2. aktywność złośliwego oprogramowania,
    3. aktywność użytkowników i wykorzystanie kont,
    4. zmiany w zawartości krytycznych obiektów systemowych,
    5. stan zainstalowanych poprawek/patchy dla oprogramowania systemowego,
    6. informacje o ruchu sieciowym,
    7. informacje dotyczące ataków sieciowych,
    8. wykorzystanie dostępu do Internetu przez pracowników,
    9. wykryte podatności na podstawie raportów skanerów podatności,
    10. zmiany w konfiguracji urządzeń sieciowych,
    11. aktywność użytkowników (na podstawie tożsamości),
    12. raporty dotyczące obsługi incydentów przez operatorów systemu,
    13. raporty dotyczące wykrycia wskaźników kompromitacji.
19. System SIEM musi pozwalać na definiowanie własnych i modyfikację istniejących raportów, zapytań i dashboardów dostarczonych przez producenta.
20. System SIEM musi umożliwiać podejmowanie automatycznych akcji lub alarmowania. Dostępne akcje muszą obejmować:
    1. utworzenie incydentu w Systemie,
    2. wysłanie email,
    3. uruchomienie skryptu i przekazanie parametrów wywoławczych,
    4. integrację z systemami klasy service-desk,
    5. integrację z systemami klasy SOAR,
    6. modyfikacja list kontrolnych.
       1. Rozwiązanie musi zawierać API pozwalającą na budowanie nowych akcji, w tym przekazanie wybranych pól zdarzenia jako parametrów akcji.
21. System SIEM musi umożliwiać jednoczesną wielostanowiskową pracę analityczną co najmniej dla 10-ciu użytkowników.
22. System SIEM powinien cechować się uniwersalnością, tzn. oprócz funkcjonalności dedykowanych bezpieczeństwu, powinien zapewniać możliwość wykorzystania wybranego rozwiązania do analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych.
23. System SIEM musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych obejmujących:
    1. mechanizmy pobierania danych,
    2. raporty, dashboardy i formularze,
    3. nowe funkcje analityczne,
    4. nowe sposoby wizualizacji,
    5. mechanizmy powiadamiania, w tym dwukierunkowe - inne niż przewidział producent.

Realizacja tych funkcjonalności nie może wymagać konieczności angażowania Producenta i nie może naruszać praw autorskich. Komponenty oferowanego rozwiązania w obszarze analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych nie muszą pochodzić od jednego Producenta, jednak nie mogą być to rozwiązania open source.

# Wymagania techniczne i bezpieczeństwa

1. Komunikacja użytkownika z systemem SIEM musi odbywać się przy użyciu przeglądarki internetowej (wsparcie dla co najmniej: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome). Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java, OpenJDK, JRE lub Microsoft Silverlight.
2. Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi takich klient SSH lub RDP.
3. System SIEM powinien umożliwiać komunikację z nim za pomocą urządzeń mobilnych Apple IOS i Google Android i pozwalać na integrację alarmów z powiadomieniami na ww. urządzenia.
4. System SIEM musi zostać dostarczony w konfiguracji zapewniającej odporność na awarię w zakresie komponentu przechowującego dane – klaster złożony z co najmniej 2 węzłów.
5. System SIEM musi wspierać Role Based Access Control (RBAC) umożliwiając precyzyjne nadawanie uprawnień dla administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania co najmniej LDAP lub Active Directory.
6. System SIEM nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników.
7. System SIEM musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji systemu.
8. System SIEM musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck).
9. System SIEM musi umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między wszystkimi komponentami systemu.

# Wymagania funkcjonalne dla systemu SOAR - Orkiestracja i automatyzacja bezpieczeństwa

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 SOAR musi być dostarczony od tego samego Producenta co System SIEM.
3. Artefakty automatyzacji i orkiestracji muszą być tworzone za pomocą znanego języka programowania.
4. Zaawansowane funkcje i integracje platformy muszą być osiągalne za pomocą jednego języka programowania.
5. Tworzenie automatyzacji i orkiestracji musi być możliwe z poziomu graficznego interfejsu użytkownika.
6. System SOAR musi zapewniać kontrolę wersji dostępnych scenariuszy (playbooks).
7. Scenariusze muszą mieć możliwość wywoływania innych scenariuszy.
8. System SOAR musi mieć możliwość harmonogramowania uruchomienia scenariuszy.
9. System SOAR musi zapewniać uruchamianie scenariuszy automatycznych, półautomatycznych, manualnych.
10. System SOAR musi oferować wizualny debugger scenariuszy do szybkiego programowania i testowania.
11. System SOAR musi dostarczać możliwość przetestowania playbooków w trybie bezpiecznym – bez wywoływania destruktywnych działań
12. System SOAR musi posiadać możliwość definiowania scenariuszy postępowania/obsługi incydentu dla analityka (tzw. Workbooki)
13. System SOAR musi umożliwiać budowanie i dostarczanie nowych aplikacji i scenariuszy w oparciu o społeczność użytkowników.
14. System SOAR musi mieć możliwość przypisywania zadań w cyklu realizacji scenariusza do różnych analityków z możliwością śledzenia realizacji zadań.
15. System SOAR musi umożliwiać tworzenie przypomnień dla zadań.
16. System SOAR musi być zbudowany jako dedykowany silnik automatyzacji bezpieczeństwa, a nie ogólny silnik automatyzacji.
17. System SOAR musi przedstawiać analitykom sugestie dotyczące dalszych działań uwzględniające kontekst, w oparciu o działania, które inni analitycy wybrali w podobnych sytuacjach w przeszłości.
18. System SOAR musi oferować gotowe integracje z rozwiązaniami bezpieczeństwa dostępnymi na rynku. Gotowe integracje muszą zawierać przygotowane do użycia akcje.
19. System SOAR musi korzystać z rynkowych standardów normalizacji, takich jak np. common event framework.
20. System SOAR musi mieć możliwość wzbogacania danych ze źródeł zewnętrznych, w szczególności z Systemu SIEM.
21. System SOAR musi zapewniać możliwość wprowadzania informacji od analityków do przepływów pracy.
22. System SOAR musi mieć możliwość przyjmowania informacji poprzez email.
23. System SOAR powinien mieć możliwość integracji z zewnętrznymi źródłami reputacji, informacji o zagrożeniach itp. poprzez interfejs TAXII/STIX np. Threat Intel Platforms (TIP).
24. System SOAR musi zapewnić możliwość uruchomienia wielu playbooków na tych samych zdarzeniach, bez nadpisywania wyników wcześniej uruchomionych playbooków.

# Zarządzanie Incydentami w Systemie SOAR

1. Zarządzanie incydentami musi być integralną częścią Systemu.
2. System SOAR musi mieć możliwość grupowania incydentów w ramach sprawy.
3. System SOAR musi umożliwiać współpracę pomiędzy analitykami bezpieczeństwa w czasie rzeczywistym.
4. Każdy incydent musi posiadać unikalny identyfikator.
5. System SOAR musi umożliwiać współpracę między departamentami do rozwiązywania incydentów poprzez nadawanie specjalnych uprawnień do poszczególnych zgłoszeń.
6. System SOAR musi mieć możliwość zmiany krytyczności incydentu w oparciu o zdefiniowane kryteria.
7. System SAOR musi mieć możliwość automatycznego eskalowania zgłoszeń w oparciu o zdefiniowane kryteria.
8. W Systemie SOAR musi istnieć funkcjonalność prowadzenia dochodzenia na incydencie, możliwości korelacji incydentów, dołączania artefaktów, przeglądania i podpinania innych incydentów.
9. System SOAR musi posiadać funkcjonalność zarządzania sprawami, pozwalającą na rekonstrukcję wykonanych działań, podjętych decyzji, raportowania realizacji dochodzenia.
10. Musi istnieć możliwość tagowania incydentów informacjami o atakujących lub wskaźnikami zagrożenia.
11. Rekord incydentu musi umożliwiać rejestrację co najmniej poniższych atrybutów incydentu:
    1. numer sprawy,
    2. opis sprawy,
    3. priorytet,
    4. eskalacja,
    5. kategoria,
    6. status,
    7. treść sprawy,
    8. odnośniki do zewnętrznych obiektów,
    9. załączniki.
12. System SOAR musi umożliwiać śledzenie parametrów SLA incydentów
13. System SOAR musi umożliwiać pełną lub częściową automatyczną analizę incydentu.
14. System SAOR musi udostępniać funkcjonalność war-room w celu usprawnienia współpracy pomiędzy analitykami i zespołami.
15. System SOAR musi umożliwiać integrację z rozwiązaniami IT Service Management.
16. System SOAR musi dawać analitykowi możliwość uruchomienia wielu playbooków na tych samych zdarzeniach, bez nadpisywania wyników wcześniej uruchomionych playbooków
17. System SOAR musi posiadać tryb debagowania playbooków z możliwością generowania zdarzenia testowe, bez konieczności działań na prawdziwych danych.
18. System SOAR posiada wbudowane mechanizmy (tzw. „wtyczki”; gotowe konektory, etc.) umożliwiające automatyczną integrację z minimum 150 systemami innych producentów

# Raportowanie

1. System SOAR musi dostarczać raporty z możliwością ich dostosowania z wykorzystaniem pól z incydentu lub pól z własnym tekstem.
2. System SOAR musi umożliwiać prezentowanie raportu związanego z parametrami SLA incydentów.
3. System SOAR musi dostarczać raporty prezentujące korzyści uzyskane z automatyzacji i orkiestracji w kontekście czasu, kosztów, unikniętych zagrożeń.
4. System SOAR musi umożliwiać generowanie raportów na różnych poziomach w organizacji: poziom CISO, poziom SOC, poziom analityka bezpieczeństwa.
5. Klienci pracujący w środowiskach multi-tenant muszą mieć możliwość generowania raportów tylko dla swojej organizacji.
6. Aktywności użytkowników Systemu SIEM i Systemu SOAR musi być śledzona i logowana na potrzeby ewentualnej analizy.

# Wymagania w zakresie wydajności i pojemności

1. Dostarczony System SIEM musi umożliwiać wydajną obsługę 275000 EPS-ów, 7TB surowych danych dziennie łącznie, przy czym:
   1. dla grupy licencyjnej dedykowanej dla Ministerstwa Sprawiedliwości 6 TB surowych danych dziennie,
   2. dla grupy licencyjnej dedykowanej dla Centralnej Służby Więziennej 1 TB surowych danych dziennie,
2. System SIEM nie może mieć żadnych ograniczeń na ilość podpinanych źródeł.
3. System SIEM nie może mieć żadnych ograniczeń na ilość korelacji i IOC.
4. Przekroczenie ww. parametrów nie może skutkować żadną utratą danych. System SIEM powinien informować o takim przekroczeniu w postaci alarmu i informacji w interfejsie użytkownika.
5. W przypadku dostarczenia elementów Systemu SIEM jako dedykowane komponenty sprzętowe muszą zapewnić możliwość przechowywania danych (dane surowe i metadane) przez okres 1 roku od ich powstania.
6. System SOAR musi pozwalać na jednoczesną pracę minimum 25 operatorów łącznie, bez ograniczania ilości incydentów zarządzanych przez System SOAR w czasie, przy czym:.
   1. dla grupy licencyjnej dedykowanej dla Ministerstwa Sprawiedliwości 20 operatorów,
   2. dla grupy licencyjnej dedykowanej dla Centralnej Służby Więziennej 5 operatorów,

# Charakterystyka fizyczna (w przypadku zaoferowania fizycznych elementów Systemu SIEM lub Systemu SOAR) (jeśli dotyczy)

1. Podstawowe funkcjonalne składniki Systemu SIEM muszą umożliwiać pracę w trybie utwardzonym (rozwiązanie musi spełniać standard FIPS 140-2 Level 2).
2. System musi być zbudowany w oparciu o przygotowane przez producenta urządzenia fizyczne przeznaczone do montażu w szafie typu RACK 19”, z zainstalowanym dedykowanym oprogramowaniem (tzw. appliance). W przypadku zaoferowania Systemu opartego o środowisko wirtualne, oferowane rozwiązanie musi działać w środowisku VMware oraz Hyper-V. Niezależnie od platformy (sprzętowa czy wirtualna), System musi zapewniać wydajność i pojemność odpowiadającą posiadanym przez Zamawiającego i Jednostki licencjom na System SIEM i System SOAR przez cały okres obowiązywania Umowy.
3. Urządzenia wchodzące w skład systemu SIEM (jeżeli zaoferowano rozwiązanie oparte o sprzęt fizyczny) muszą zawierać redundantne zasilanie, system chłodzenia oraz dyski w architekturze RAID. Dopuszcza się brak redundancji zasilania w modułach pobierających dane. Architektura powinna wspierać możliwość przeprowadzania zewnętrznego backupu.
4. Urządzenia realizujące funkcje przechowywania, wyszukiwania, zarządzania bazą zebranych logów oraz analityczny, w celu przyspieszenia dostępu do danych dodatkowo powinny zawierać dyski SSD, przeznaczone do przetwarzania indeksów.

# Usługi Wykonawcy

Wszelkie usługi Wykonawcy (instalacyjno – wdrożeniowe, szkoleniowe oraz wsparcia eksperckiego wykonawcy) będą realizowane na podstawie zatwierdzonego przez Jednostkę harmonogramu, dostarczonego przez Wykonawcę, na zasadach określonych w Umowie.

Maksymalny termin wykonania Usług będzie precyzowany przez Jednostkę we Wniosku o zamówienie.

Ilości godzin będą każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług Wykonawcy, na podstawie ilości godzin wskazanych przez Jednostkę we wniosku o zamówienie.

# 13.1. Usługi Instalacyjno-Wdrożeniowe

Usługi Instalacyjno-Wdrożeniowe Systemu obejmują w szczególności:

1. Instalację i konfigurację dostarczonego Oprogramowania w tym:
   1. Wykonanie Dokumentacji, o której mowa w pkt 17 i 18 OPZ,
   2. Instalację Oprogramowania Systemu SIEM lub Systemu SOAR w środowisku Jednostki,
   3. Skonfigurowanie Systemu SIEM do potrzeb Jednostki w celu uzyskania wysokiej wydajności zgodnie z Dokumentacją projektową uzgodnioną na etapie umowy.
2. Podłączenie źródeł danych w danej lokalizacji Systemu SIEM zgodnie z Dokumentacją projektową uzgodnioną na etapie umowy.
3. Implementację tzw. play book-ów tj. wykonanie automatyzacji dla obsługi typów incydentów bezpieczeństwa (typy incydentów będą uzgodnione z Wykonawcą na etapie wdrożenia Systemu SOAR) zgodnie z Dokumentacją projektową uzgodnioną na etapie umowy.
4. Wykonanie testów akceptacyjnych wykazujących poprawność wdrożenia Systemu zgodnie z Dokumentacją projektową uzgodnioną na etapie umowy.
5. Przygotowanie procedur obsługi dot. eksploatacji, awarii, wykonania kopii zapasowych oraz ich odtworzenia, administrowania Systemu.
6. Na wniosek Wykonawcy Jednostka może wyrazić zgodę w formie dokumentowej (np. wiadomość e-mail) na wykonanie prac instalacyjno-wdrożeniowych zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Jednostkę. Jednostka ma prawo odmowy udostępnienia zdalnego dostępu w dowolnym momencie bez podawania przyczyny.
7. Ze względu na niejawność danych w zakresie posiadanych systemów oraz procedur bezpieczeństwa, szczegółowe informacje dotyczące m.in. nazw systemów czy opisy procedur bezpieczeństwa zostaną przedstawione Wykonawcy, z którym zostanie zawarta Umowa.
8. W przypadku zaoferowania Systemu innego niż obecnie wykorzystywanego przez Zamawiającego tj. rozwiązania firmy SPLUNK usługi instalacyjno – wdrożeniowe będą dodatkowo obejmować migrację do nowego Sytemu, migracja musi obejmować:
   1. Środowisko rozproszone w 13 lokalizacjach;
   2. 3 węzły centralnego przechowywania danych współdzielonych z pełną konfiguracją i restrykcjami dostępu dla poszczególnych danych przechowywanych w ww. węzłach współdzielonych.;
   3. odseparowanie danych lokalnych od współdzielonych na potrzeby dostępu do przechowywanych i przeszukiwanych zdarzeń;
   4. minimum integrację z systemami klasy:
      * Firewall
      * ThreatInteligence
      * EDR
      * AD
      * SOAR
      * Email
      * DNS
      * aplikacje własne
   5. odwzorowanie istniejących procesów analizy zdarzeń (minimum 50 korelacji)
   6. odwzorowanie istniejących procesów reakcji na zdarzenia na systemie SOAR (minimum 20 playbook)
9. Proces migracji do nowego Systemu nie może przekroczyć 15 dni roboczych oraz zostanie wykonany przez Wykonawcę na własny koszt.
10. Wykonawca przeprowadzi, na etapie wdrożenia Systemu, co najmniej 16 godzinne warsztaty szkoleniowe w języku polskim dla maksymalnie 15 uczestników w zakresie obsługi wdrażanego Systemu (instalacji, konfiguracji, administracji Systemu SIEM lub Systemu SOAR).
11. Zakres warsztatów szkoleniowych będzie precyzowany na etapie procedury wykonawczej, z zastrzeżeniem powyżej.
12. Wykonawca zapewni możliwość konsultowania z trenerami tematów omawianych podczas warsztatów szkoleniowych oraz opieki merytorycznej nad uczestnikami warsztatów w okresie 5 dni roboczych po zakończeniu warsztatów za pomocą poczty elektronicznej (udzielanie odpowiedzi drogą elektroniczną na pytania lub wątpliwości powstałe podczas warsztatów).
13. Ilości godzin usług instalacyjno-wdrożeniowych będzie każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług Wykonawcy, na podstawie ilości godzin wskazanych przez Jednostkę we wniosku o zamówienie

# Usługi Wsparcia Eksperckiego Wykonawcy

1. Usługi Wsparcia Eksperckiego Wykonawcy będą obejmowały:
   1. bieżące utrzymanie, zarządzanie i administrowanie oferowanym przez Wykonawcę Systemem,
   2. przeprowadzenie konsultacji, instruktażu, rozwiązywanie bieżących problemów związanych z obsługą, w tym instalacją, konfiguracją, optymalizacją, utrzymaniem i administracją Systemu, z wyłączeniem Awarii usuwanych w ramach Gwarancji oraz z wyłączeniem czynności wykonywanych w ramach Wsparcia Technicznego.
2. Rodzaj Usług Wsparcia Eksperckiego Wykonawcy będzie precyzowany na etapie Wniosku o zamówienie, z zastrzeżeniem pkt 1 powyżej.
3. Potwierdzeniem prawidłowej realizacji Usług Wsparcia Eksperckiego Wykonawcy, będzie podpisany bez zastrzeżeń Protokół Odbioru Usług.

# 14.Usługi szkoleniowe dostarczane przez producenta rozwiązania

Rodzaj i ilość szkoleń będzie precyzowana na etapie procedury wykonawczej, z zastrzeżeniem pkt 1-8 poniżej

Forma szkoleń: Warsztaty online prowadzone przez z wykwalifikowanego instruktora w języku polskim lub angielskim

Jednostka może zamówić dedykowane kursy szkoleniowe dostarczane przez producenta zaoferowanego rozwiązania pojedynczo dla każdej osoby, przy czym na jedno szkolenie Jednostka może wysłać więcej niż jedną osobę w tym samym czasie. Jednostka może zamówić maksymalnie 29 takich samych szkoleń (przez jedno szkolenie rozumie się jedno szkolenie dla jednej osoby) z każdego z ośmiu zakresów szkoleń opisanych poniżej (pogrupowanych w 8 dedykowanych zakresów tematycznych):

1. Szkolenie w wymiarze min. 12 godzin, dedykowane administratorom odpowiedzialnym za zarządzanie środowiskiem SIEM.

Ma dostarczyć wiedzy z zakresu obsługi licencji, serwerów pełniących rolę bazodanową (indeksującą) oraz serwerów służących do wyszukiwania / analizy informacji pozyskiwanych z serwerów bazodanowych.

Swoim zakresem ma pokrywać konfigurację, zarządzanie oraz monitoring środowiska SIEM.

Opis:

* 1. omówienie wdrażania systemu SIEM,
  2. zarządzanie licencjami,
  3. omówienie konfiguracji,
  4. omówienie możliwości rozszerzania funkcjonalności systemu SIEM
  5. zarządzanie serwerami bazodanowymi / indeksującymi,
  6. zarządzanie rolami, użytkownikami oraz rodzajami autoryzacji,
  7. podstawowe mechanizmy przekierowania źródeł danych,
  8. omówienie wyszukiwania rozproszonego

1. Szkolenie w wymiarze min. 18 godzin, dedykowane administratorom odpowiedzialnym za konfigurowanie źródeł danych dla systemu SIEM.

Ma dostarczyć wiedzy z zakresu serwerów pełniących rolę przekierowującą logi ze źródeł do serwerów bazodanowych / indeksujących.

Swoim zakresem ma pokrywać instalację, konfigurację, zarządzanie, monitoring i rozwiązywanie problemów serwerów przekazujących dane oraz środowiska SIEM.

Opis:

* 1. Wyjaśnienie znaczenia rodzajów / typów danych,
  2. Wdrażanie i zarządzanie serwerami przekierowującymi dane,
  3. Omówienie typów i konfiguracji możliwych do podłączenia źródeł danych,
  4. Omówienie źródeł danych pod kątem prawidłowego ich rozpoznawania / parsowania,

1. Szkolenie w wymiarze min. 3 godzin, dedykowane zaawansowanym użytkownikom chcącym nauczyć się jak obliczać zależności pomiędzy polami z różnych źródeł danych.

Opis:

1. Praktyczne korzystanie z poleceń umożliwiających dodawanie pól, złączenia, dodawanie kolumn do uzyskanych wyników

Forma szkolenia: Warsztaty online z laboratorium

1. Szkolenie w wymiarze min. 13 godzin, dedykowane osobom projektującym rozwiązania SIEM oraz administratorom, przygotowujące do instalowania i konfiguracji rozwiązań SIEM.

Ma dostarczać wiedzy z zakresu obsługi zdarzeń, wdrażania wymagań, możliwych aplikacji dodatkowych, tworzenia dashboardów, zarządzania ryzykiem i dopasowywanie informacji o zagrożeniach

1. Szkolenie w wymiarze min. 3 godzin, dedykowane dla administratorów, celem przygotowania do używania środowiska SOAR pod kątem odpowiedzi na incydenty, analizy zagrożeń oraz wykonywania akcji mitygacyjnych i przeciwdziałającym zagrożeniom bezpieczeństwa.

Opis:

1. Koncepcja środowiska SOAR,
2. Analiza,
3. Uruchamianie akcji i playbooków,
4. Zarządzanie zdarzeniami i przepływem danych
5. Szkolenie w wymiarze min. 3 godzin, dedykowane dla administratorów, celem przygotowania do konfiguracji i zarządzania środowiskiem SOAR.

Opis:

1. Koncepcja środowiska SOAR,
2. Wstępna konfiguracja,
3. Konfiguracja automatyzacji,
4. Zarządzanie użytkownikami,
5. Importowanie danych,
6. Dostosowywanie i monitoring środowiska
7. Szkolenie w wymiarze min. 9 godzin, dedykowane dla administratorów celem przygotowania do planowania, projektowania, tworzenia i analizy playbooków w środowisku SOAR.

Uczestnicy mają poznać możliwości, sposób tworzenia oraz testowania playbooków.

Opis:

1. Automatyzacja najlepszych praktyk,
2. Tworzenie playbooków automatyzacji i wprowadzania danych,
3. Korzystanie z akcji i decyzji,
4. Wykorzystywanie wyników akcji,
5. Testowanie i analiza playbooków,
6. Interakcja z użytkownikami,
7. Formatowanie danych wyjściowych,
8. Kompleksowa logika środowiska,
9. Praca z wykorzystaniem artefaktów,
10. Wykorzystywanie plików w pracy z playbookami,
11. Tworzenie własnych list,
12. Filtrowanie danych
13. Szkolenie w wymiarze min. 13 godzin, dedykowane dla osób posiadających doświadczenie w pracy ze środowiskiem SOAR. Przygotowuje do tworzenia złożonych rozwiązań SOAR łącznie z integracją środowiska SOAR z środowiskiem SIEM, a także opracowywania playbooków wymagających niestandardowego przygotowania oraz używania REST API.

Opis:

1. Korzystanie z wyszukiwań zewnętrznych,
2. Przesyłanie zdarzeń z środowiska SIEM do SOAR,
3. Aktualizowanie przy pomocy systemu SOAR zdarzeń w środowiskach SIEM,
4. Uruchamianie playbooków systemu SOAR z poziomu SIEM,
5. Przeszukiwanie danych znajdujących się w środowisku SIEM przy użyciu playbooków systemu SOAR,
6. Przygotowywanie niestandardowego kodu do wykorzystania w playbookach systemu SOAR,
7. Korzystanie z REST API w playbookach systemu SOAR,

# 15 Wymagania w zakresie Gwarancji i wsparcia technicznego na System SIEM i System SOAR

1. Jednostka udostępni dedykowany system zgłoszeń umożliwiający zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego Awarii. Wykonawca w ramach udzielonej Gwarancji zobowiązany będzie do obsługi Zgłoszeń Serwisowych za pośrednictwem ww. oprogramowania, wdrożonego w strukturze Odbiorcy i Jednostek.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie SIEM i Systemie SOAR nie mogą skutkować utratą praw gwarancyjnych do Systemu SIEM i Systemu SOAR.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe awarii Systemu SIEM lub Systemu SOAR w następujący sposób:
   1. **Awaria Krytyczna** - wada skutkująca nieprawidłowym działaniem Systemu SIEM lub Systemu SOAR powodująca albo całkowity brak możliwości korzystania z Systemu SIEM lub Systemu SOAR przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje tj. zarządzania zdarzeniami i informacjami bezpieczeństwa lub automatyzacji i strukturyzacji procesów w systemach informatycznych: Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Jednostkę, Czas Naprawy do 24 godzin od chwili Zgłoszenia Serwisowego;
   2. **Awaria Niekrytyczna** - wada skutkująca nieprawidłowym działaniem Systemu SIEM lub Systemu SOAR powodująca ograniczenie korzystania z Systemu SIEM lub Systemu SOAR, nie powodując skutków opisanych dla Awarii Krytycznej: Czas Reakcji do 4 godzin od chwili Zgłoszenia Serwisowego przez Jednostkę, Czas Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego.
4. Wszelkie awarie będą zgłaszane przez Jednostkę za pomocą oprogramowania, o którym mowa w punkcie 1 powyżej.
5. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:
   * 1. aktualizację i konfigurację Systemu SIEM lub Systemu SOAR przez Wykonawcę,
     2. rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu SIEM lub Systemu SOAR.
     3. Wykonawca w ramach udzielonej gwarancji na wezwanie i w terminie uzgodnionym z Jednostką zainstaluje poprawki, usprawnienia i nowe wersje Oprogramowania dla Systemu, udostępniane przez producenta wdrożonego Systemu SIEM lub Systemu SOAR.
6. W ramach udzielonego wsparcia technicznego Jednostkom przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu SIEM lub Systemu SOAR udostępnianych przez producenta Systemu SIEM lub Systemu SOAR bez ponoszenia dodatkowych kosztów finansowych przez Jednostki. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Jednostkom.
7. Świadczenia gwarancyjne w zakresie Sprzętu (o ile dotyczy – jeżeli Wykonawca oferuje rozwiązanie oparte o Sprzęt fizyczny) realizowane będą z uwzględnieniem następujących zasad:
   1. usługi gwarancyjne będą świadczone przez producenta Sprzętu lub podmiot posiadający autoryzację producenta Sprzętu, w miejscu użytkowania Sprzętu, jeśli jednak naprawa Sprzętu w tym miejscu okaże się niemożliwa, naprawa może zostać wykonana w innym miejscu; usługi gwarancyjne Sprzętu będą świadczone w Dni Robocze, w godzinach od 8:00 do 16:00;
   2. w zakres usług gwarancyjnych wchodzi również dojazd i praca osób wykonujących czynności gwarancyjne w imieniu Wykonawcy oraz pozostałe koszty niezbędne do świadczenia usług gwarancyjnych, w tym koszty dostawy i odbioru wymienionych urządzeń, niezależnie od podmiotu wykonującego usługę gwarancyjną;
   3. na czas naprawy Sprzętu poza miejscem jego użytkowania Sprzęt zabierany będzie bez dysku twardego lub innych elektronicznych nośników informacji (o ile dotyczy). Po zwrocie naprawionego sprzętu dysk twardy lub inne elektroniczne nośniki informacji zostaną ponownie zamontowane przez Wykonawcę, po czym nastąpi sprawdzenie poprawności funkcjonowania naprawionego Sprzętu;
   4. w przypadku nieodwracalnej awarii dysku twardego lub innych elektronicznych nośników informacji (o ile dotyczy) będą one wymienione przez Wykonawcę na nowy, wolny od wad, o parametrach nie gorszych niż te, które uległy awarii. Uszkodzony dysk twardy lub inne elektroniczne nośniki informacji nie będzie podlegał zwrotowi Wykonawcy;
   5. Wykonawca zobowiązuje się zapewnić, że każda osoba wykonująca usługi gwarancyjne w miejscu wykorzystywania Sprzętu, będzie posiadała dokument tożsamości i pisemne upoważnienie do wykonywania napraw i czynności objętych gwarancją, potwierdzone przez Wykonawcę oraz będzie zobligowana stosować się do przepisów wewnętrznych Jednostki dotyczących ruchu osobowego i materiałowego w jej siedzibie;
   6. Usługi gwarancyjne wykonywane będą przy wykorzystaniu materiałów, sprzętu i narzędzi Wykonawcy, chyba że naprawa zostanie wykonana w punkcie serwisowym producenta nie będącego Wykonawcą;
   7. Części lub podzespoły, które zostaną wymienione w ramach usług gwarancyjnych stają się własnością Wykonawcy, który zobowiązuje się do ich bezpośredniego odbioru od Jednostek i utylizacji zgodnie z obowiązującymi przepisami;
   8. W przypadku wymiany części lub podzespołów, Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną dla wymienionych elementów Sprzętu, (jeżeli ich producent udziela odrębnej gwarancji);
   9. W przypadku niemożności dotrzymania terminu naprawy Sprzętu, Wykonawca zobowiązany jest do dostarczenia w pierwszym Dniu Roboczym po upływie tego terminu, na swój koszt, do siedziby Jednostki, Sprzętu zastępczego o parametrach nie gorszych niż Sprzęt, który podlega naprawie, na cały okres naprawy Sprzętu, posiadającego stosowne certyfikaty/ dokumenty;
   10. W razie niedokonania naprawy Sprzętu (usunięcia awarii) w terminie:
       1. dopuszcza się dokonanie naprawy siłami własnymi Zamawiającego lub Jednostki na koszt Wykonawcy lub zlecenie naprawy osobie trzeciej na koszt Wykonawcy, z zachowaniem praw wynikających z Gwarancji i rękojmi za wady Sprzętu, bez dodatkowego wezwania Wykonawcy do wykonania usługi gwarancyjnej. W przypadku skorzystania z powyższego uprawnienia, Wykonawca zostanie niezwłocznie powiadomiony w formie pisemnej o tym fakcie oraz zakresie zleconych prac (napraw, zmian, itp.). W takim przypadku Wykonawca zobowiązany jest zapłacić Jednostce – w terminie wskazanym przez tę Jednostkę, nie krótszym jednak niż 14 dni kalendarzowych – kwotę stanowiącą równowartość poniesionego przez Jednostkę kosztów wykonania tych prac.
       2. okres Gwarancji przedłuża się o czas trwania naprawy, a w przypadku gdy ten sam element Sprzętu po raz trzeci ulegnie awarii podlegającej naprawie gwarancyjnej, Wykonawca zobowiązany jest dokonać wymiany elementu Sprzętu na nowy, o takich samych lub lepszych funkcjonalnościach oraz takich samych lub lepszych parametrach, bez dodatkowego wezwania Wykonawcy. Wymiana Sprzętu na nowy powinna zostać potwierdzona protokołem, który zawierał będzie co najmniej datę dostawy nowego Sprzętu. W takiej sytuacji termin gwarancji biegnie na nowo od chwili dostarczenia i potwierdzenia protokolarnego dostawy nowego Sprzętu.
   11. Rozbudowa lub modyfikacje Sprzętu nie mogą prowadzić do utraty uprawnień wynikających z rękojmi za wady urządzenia lub utraty prawa do korzystania z usług gwarancyjnych.

### 16. Dokumentacja Projektowa

Dokumentacja Projektowa ma zawierać, w szczególności:

* 1. Opis funkcjonalny Systemu SIEM lub Systemu SOAR,
  2. Szczegółowy wykaz wymaganych elementów, sposób ich wdrożenia i konfiguracji, wykaz licencji i Sprzętu (o ile dotyczy), potrzebnych do realizacji projektu, wraz ze specyfikacją techniczną,
  3. Szczegółowy opis architektury Systemu wraz z planem oraz z opisem integracji z infrastrukturą techniczną Jednostki,
  4. Harmonogram wdrożenia, zgodny z wymogami Umowy,
  5. Dokumentację Testów Akceptacyjnych wdrożenia Systemu SIEM lub Systemu SOAR, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System SIEM lub Systemu SOAR jest zgodny z opisem przedmiotu zamówienia oraz w zakresie objętym umową. Testy akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez Jednostkę na etapie odbioru Dokumentacji Projektowej.
  6. Dokumentacja Projektowa powinna być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być dostarczone w języku angielskim lub polskim.

### 17. Dokumentacja Powykonawcza

Dokumentacja Powykonawcza ma zawierać, w szczególności:

1. Szczegółową konfigurację oraz opis infrastruktury technicznej Systemu SIEM lub Systemu SOAR,
2. Opis struktury i konfiguracji Systemu, w tym pliki konfiguracyjne, skrypty uruchomieniowe, skrypty zatrzymujące, itp.,
3. Zalecenia i procedury eksploatacyjne oraz zalecenia w zakresie konserwacji Systemu, w tym przeglądu logów wraz z procedurami.
4. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu SIEM lub Systemu SOAR, w szczególności:
   1. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu SIEM lub Systemu SOAR,
   2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
   3. instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
   4. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu SIEM lub Systemu SOAR, uzgodnione z przedstawicielem Zespołu Odbiorowego.
5. Dokumentacja Powykonawcza powinna być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być dostarczone w języku angielskim lub polskim.

### 18 Wymagania w zakresie Personelu Kluczowego niezbędnego do realizacji Umów

* + - 1. Zamawiający wymaga, aby przez cały okres obowiązywania Umowy Wykonawca dysponował odpowiednim personelem, w tym Personelem Kluczowym, spełniającym następujące wymagania:

1. **co najmniej jednym** kierownikiem projektu posiadającym minimum 3-letnie doświadczenie w zakresie wdrażania lub projektowania Systemów klasy SIEM jako kierownik projektu lub architekt rozwiązań; posiadającym certyfikat w zakresie bezpieczeństwa informacji - vendor-neutral (np: CompTIA Security+, CISSP – Certified Information Systems Security Professional, CISM - Certified Information Security Manager lub równoważne);
2. **co najmniej dwoma** Specjalistami Wdrożeniowymi, z których każdy w ciągu ostatnich 3 lat przed złożeniem odpowiedzi na Wniosek o zamówienie pełnił funkcję polskojęzycznego specjalisty wdrożeniowego w co najmniej 2 projektach informatycznych dotyczących wdrażania oferowanego systemu SIEM oraz Systemu SOAR; z których każdy posiada:
   1. certyfikaty producenta oferowanego Systemu SIEM oraz Systemu SOAR na poziomie minimum Architect lub certyfikat wydany przez producenta oferowanych Systemów SIEM i SOAR potwierdzający kompetencje w zakresie wdrażania i opracowywania ich Architektury.
3. co najmniej dwoma Specjalistami ds. bezpieczeństwa, posiadającymi znajomość zagadnień, rozwiązań i narzędzi w zakresie projektowania i budowania rozwiązań bezpieczeństwa na potrzeby systemów informatycznych, potwierdzone przynajmniej jednym z poniższych certyfikatów: CISSP - Certified Information System Security Professional, CISA - Certified Information System Auditor, CISM - Certified Information System Manager lub innymi równoważnymi potwierdzającymi posiadanie umiejętności w wyżej wymienionym zakresie oraz doświadczenie wynikające z udziału, w co najmniej jednym przedsięwzięciu w charakterze specjalisty ds. bezpieczeństwa systemów informatycznych zakończonym w okresie ostatnich 3 lat przed upływem terminu składania ofert.
   * + 1. Jednostka na etapie procedur wykonawczych określi we Wniosku o zamówienie wymaganą ilość Personelu Kluczowego, spośród osób wymienionych powyżej, niezbędnych do realizacji danego zamówienia, w zależności od stopnia jego złożoności (o ile dotyczy).
       2. Wykonawca w odpowiedzi na Wniosek o zamówienie wskaże osoby skierowane do realizacji danego zamówienia oraz określi ich doświadczenie i kwalifikacje, przy czym jedna osoba może być wskazana do pełnienia maksymalnie dwóch funkcji.
       3. Na żądanie Jednostki, najpóźniej na 2 dni przed rozpoczęciem świadczenia Usług przez Personel Kluczowy, Wykonawca przedstawi potwierdzone za zgodność z oryginałem kopie wymaganych certyfikatów.