# **Szczegółowy opis przedmiotu zamówienia**

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

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

oraz

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

wraz ze wsparciem technicznym, Gwarancją oraz Usługami w maksymalnej łącznej ilości 3000 godzin zegarowych do wykorzystania w całym okresie realizacji, obejmującymi: usługi instalacyjno-wdrożeniowe, warsztaty szkoleniowe oraz Usługi Rozwoju Systemu (konfiguracje   
i optymalizacje). Zamawiający przewiduje możliwość wdrożenia kilku instancji Systemu w różnych lokalizacjach, konfiguracjach i różnym czasie dostawy w trakcie obowiązywania Umowy.

# 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. System SIEM musi posiadać wsparcie techniczne producenta. Nie dopuszcza się rozwiązań open source.
2. System SIEM musi istnieć na rynku co najmniej 5 lat 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 usług,
   2. wydajności aplikacji.
4. System SIEM musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych obejmujące:
   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.
6. Licencja musi dopuszczać dowolne kształtowanie architektury Systemu SIEM, w szczególności stosowanie dowolnej liczby komponentów poszczególnych funkcji opisanych w punkcie powyżej. Rozbudowa Platformy 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 na instalację dodatkowych instancji Systemu SIEM i Systemu SOAR oraz dowolne przypisywanie posiadanych licencji pomiędzy tymi instancjami jak również łączenie w jedną większą instancję (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. Nie dopuszcza się komponentów w wersjach beta.
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 multi-tenant.
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 producenta przez okres 36 miesięcy. W ramach udzielonego wsparcia technicznego Zamawiającemu 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 Zamawiającego.
16. Wykonawca dostarczy Oprogramowanie wraz z licencjami do korzystania z Systemu SIEM oraz Systemu SOAR w liczbie niezbędnej do budowy i uruchomienia Systemu.
17. Wykonawca dostarczy najnowsze wersje Oprogramowania dla elementów Systemu SIEM oraz 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 z co najmniej z następujących systemów i aplikacji:
   1. Systemy Windows 2003/2008/2012 oraz XP/7/8.x/10.
   2. Systemy Linux (każda dystrybucja)
   3. Urządzanie sieciowe Cisco, Nortel, Alcatel, MikroTik, Juniper, Fortinet
   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. trap SNMP
   3. 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)
   4. pliki tekstowe,
   5. logi JMS, JMX,
   6. dane z systemów wirtualizacji,
   7. dane z systemów chmurowych,
   8. NetFlow v5 i v9, sFlow, jFlow, IPFIX,
   9. 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 Zamawiający będzie chciał 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. parametry urządzeń pobierane z wykorzystaniem SNMP v2c/3,
    2. dane wydajnościowe Windows Performance Monitor,
    3. dowolne dane WMI,
    4. wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym,
    5. Zmiany w zawartości plików i kluczy rejestrów.
    6. 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. 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 tworzenie parserów. Nazwy pól powinny być określone strukturą XML
   2. System SIEM musi umożliwiać obsługę logów w formacie CEF bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą CEF.
   3. System SIEM musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą JSON.
   4. System SIEM musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie 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 zaciągania danych historycznych (już istniejących w bazie danych proponowanego rozwiązania) lub przebudowywania bazy zdarzeń.

# 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 możliwe w oparciu o te same narzędzia.
2. System SIEM musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów ww. klastra w celi 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 samodzielnie zarządzać retencją danych. Wymagana jest obsługa co najmniej dwóch etapów życia danych: WARM i COLD. Z każdym etapem związane jest miejsce przechowywania danych. Migracja danych musi następować automatycznie po określonym czasie (wiek danych) lub osiągnięciu określonej objętości. Musi istnieć możliwość stworzenie różnych schematów retencji dla różnych typów danych. Dane COLD muszą być dostępne w ten sam sposób co dane WARM, w szczególności nie jest dopuszczalne wymaganie jakichkolwiek czynności związanych z odtwarzaniem danych COLD.
4. 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.
5. 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.

# 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, JPG.
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. Rozwiązania 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 misi 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 tworzenie 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 tworzenie 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 istnienie incydentu.
9. W systemie SIEM musi istnieć możliwość pracy nad jednym incydentem więcej niż jednemu analitykowi naraz. Każda akcja wykonana przez poszczególnego analityka musi być odnotowana na timeline incydentu (do analizy dla przełożonych).
10. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto.
11. Musi istnieć możliwość prezentacji opisu zasobu w postaci serwera lub stacji roboczej obejmującego: 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.
12. 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.
13. 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. Facebook Threatconnect
    5. System musi również interpretować pliki w formacie CSV, STIX, OpenIOC, tekstowym interpretowanym z wykorzystaniem REGEX.
14. 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 samodzielnie przez administratora.
15. Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach.
16. 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.
17. System SIEM musi pozwalać na definiowanie własnych i modyfikację istniejących raportów, zapytań i dashboardów dostarczonych przez producenta.
18. System SIEM musi umożliwiać podejmowanie automatycznych akcji lub alarmowanie. 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. modyfikacja list kontrolnych.
       1. Rozwiązanie musi zawierać API pozwalająca na budowanie nowych akcji w tym przekazanie wybranych pól zdarzenia jako parametrów akcji.
19. System SIEM musi umożliwiać́ na jednoczesną wielostanowiskową pracę analityczną co najmniej dla 10-ciu użytkowników.
20. System SIEM powinien cechować się uniwersalnością, tzn. oprócz funkcjonalności dedykowanych bezpieczeństwu, powinno zapewniać możliwość wykorzystania wybranego rozwiązania do analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych.
21. 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 1 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: Internet Explorer, Firefox, 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 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. healtcheck).
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, pół-automatycznych, manualnych
10. System SOAR musi oferować wizualny debugger scenariuszy do szybkiego programowania i testowania.
11. System SOAR musi umożliwiać budowanie i dostarczanie nowych aplikacji i scenariuszy w oparciu o społeczność użytkowników.
12. System SOAR musi zawierać wiele gotowych, dostępnych natywnie w systemie scenariuszy orkiestracji.
13. System SOAR musi mieć możliwość przypisywania zadań w cyklu realizacji scenariusza do różnych analityków z możliwością śledzenia realizacji zadań.
14. System SOAR musi umożliwiać tworzenie przypomnień dla zadań.
15. System SOAR musi być zbudowany jako dedykowany silnik automatyzacji bezpieczeństwa, a nie ogólny silnik automatyzacji.
16. System SOAR musi przedstawiać analitykom sugestie dotyczące dalszych działań uwzględniające kontekst, w oparciu o działania, które inni analitycy wybrali w podobnych sytuacjach w przeszłości.
17. System SOAR musi oferować gotowe integracje z rozwiązaniami bezpieczeństwa dostępnymi na rynku. Gotowe integracje muszą zawierać przygotowane do użycia akcje.
18. System SOAR musi korzystać z rynkowych standardów normalizacji, takich jak np. common event framework.
19. System SOAR musi mieć możliwość wzbogacania danych ze źródeł zewnętrznych w szczególności z Systemu SIEM
20. System SOAR musi zapewniać możliwość wprowadzania informacji od analityków do przepływów pracy.
21. System SOAR musi mieć możliwość przyjmowania informacji poprzez email
22. System SOAR powinien mieć możliwość integracji z zewnętrznymi źródłami reputacji, informacji o zagrożeniach itp. poprzez interfejs TAXII/STIX np. Threat Intel Platforms (TIP).

# 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. Rozwiązanie musi umożliwiać współpracę między departamentalną 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 możliwością 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

# 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 SIAEM 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 42000 EPS-ów , 900 GB surowych danych dziennie.
2. System SIEM nie może mieć żadnych ograniczeń na źródeł podpinanych źródeł.
3. System SEIM 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 5 operatorów, bez ograniczania ilości incydentów zarządzanych przez System SOAR w czasie.

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

1. Podstawowe funkcjonalne składniki rozwiązania SIEM muszą umożliwiać pracę w trybie utwardzonym (rozwiązanie musi spełniać standard FIPS 140-2 Level 2).
2. System musi być zbudowany 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. Niezależnie od platformy (sprzętowa czy wirtualna), System musi zapewniać wydajność i pojemność odpowiadającą posiadanym przez Zamawiającego 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 Rozwoju Systemu

1. Usługi Rozwoju Systemu będą obejmowały, konfigurowanie oraz optymalizację Systemu SIEM oraz Systemu SOAR, a także konsultacje w zakresie obsługi generowanych zdarzeń przez system SIEM oraz System SOAR.
2. Zlecenia Usług Rozwoju Systemu oraz ich zakres będzie każdorazowo uzgadniany i rozliczany z puli godzin przeznaczonej na świadczenie Usług.