WAG.II.261.1.12 .2020

Kraków, 5 lutego 2021 roku

Uczestnicy postępowania o udzielenie zamówienia publicznego na „Rozbudowę systemu SIEM Splunk Enterprise”

Narodowy Fundusz Zdrowia - Małopolski Oddział Wojewódzki Narodowego Funduszu Zdrowia w Krakowie, w odpowiedzi na pytania wykonawcy dotyczące ogłoszenia udziela odpowiedzi jak poniżej.

Pytanie nr 1

Zamawiający w Opisie Przedmiotu Zamówienia dopuszcza możliwość instalacji systemu SIEM równoważnego „w przypadku zachowania parametrów użytkowych, funkcjonalnych i jakościowych, które będą na poziomie nie niższym od parametrów wskazanych przez Zamawiającego w punkcie I i II oraz posiadanego przez Zmawiającego systemu SIEM Splunk Enterprise Perpetual 20GB/day (licencja wieczysta)."

Splunk Enterprise pozycjonowany jest jako jeden z liderów w zestawieniu Gartner Magie Quadrant 2020. Proszę o potwierdzenie, że Zamawiający uzna parametry użytkowe, funkcjonalne i jakościowe za zachowane jeżeli dostarczony system będzie pozycjonowany również jako lider w powyższym zestawieniu. W przeciwnym razie proszę o podanie konkretnych parametrów użytkowych, funkcjonalnych i jakościowych, które będą podlegały porównaniu.

Odpowiedź:

Oferowany równoważny system SIEM musi spełniać wszystkie wymogi opisane w załączniku nr 1 do specyfikacji istotnych warunków zamówienia dotyczących licencji, subskrypcji, wsparcia serwisowego dla nowych licencji oraz posiadanego systemu SIEM. Równoważny system SIEM musi zapewnić podstawowe wymagania opisane w punktach 1-8 oraz szczegółowe wymagania przedstawione w tabeli poniżej.

Podstawowe wymagania dla oferowanego równoważnego systemu SIEM:

1. wykrywanie awarii i innych problemów na podstawie logów i metryk pozyskiwanych z urządzeń i systemów informatycznych.
2. weryfikacja funkcjonowania zasad bezpieczeństwa i stosowanych środków kontrolnych,

Małopolski Oddział Wojewódzki, ul. Józefa 21, 31-056 Kraków
tel.: 012 298 81 00, fax: 012 430 64 40, e-mail: sekretariat@nfz-krakow.pl

3. zapewnienie mechanizmów monitorujących pracowników i innych użytkowników infrastruktury teleinformatycznej,
4. podział obowiązków w zakresie monitorowania i rozliczania użytkowników uprzywilejowanych,
5. monitorowanie funkcjonowania aplikacji i urządzeń w celu szybszego reagowania na możliwe problemy i awarie,
6. zarządzanie wykrywaniem, priorytetyzowaniem i rozwiązywaniem incydentów bezpieczeństwa,
7. zbieranie, zapisywania i przechowywanie logów na czas określony przez prawo i regulaminy wewnętrzne. Dane muszą być; przechowywane w sposób zapewniający ochronę ich integralności,
8. korelacji informacji pochodzących z różnych źródeł w celu wykrycia zaawansowanych zagrożeń i/lub eliminacji fałszywych alarmów

Szczegółowe wymagania dla oferowanego równoważnego systemu SIEM:

LP	Wymagania
1. Wymagania ogólne	
1.1.	System musi realizować funkcjonalność systemu zarządzania informacją i zdarzeniami bezpieczeństwa SIEM. Oferowane rozwiązanie musi znajdować się w kwadrancie liderów Magic Quadrant for Security Information and Event Management (SIEM) Gartnera w edycji najbardziej aktualnej na dzień składania ofert.
1.2.	System musi umożliwiać wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie monitorowania usług IT, wydajności aplikacji, monitorowania usług.
1.3.	System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych za analizą danych obejmujące: a) mechanizmy pobierania danych, b) raporty, dashboardy i formularze, c) nowe funkcje analityczne, d) nowe sposoby wizualizacji, e) mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent. Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta i nie może naruszać praw autorskich.

1.4.	Architektura systemu musi umożliwiać rozdzielenie na osobne serwery funkcji: pobierania danych, przechowywania, wyszukiwania i zarządzania bazą zebranych logów, warstwy analitycznej i interfejsu użytkownika.
1.5.	Licencja musi dopuszczać dowolne kształtowanie architektury systemu, 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 kosztami licencyjnymi.
2. Wymagania funkcjonalne - pozyskiwanie danych	
2.1.	System musi umożliwiać pobieranie logów/zdarzeń z dowolnych systemów i urządzeń. Na etapie wdrożenia należy zapewnić wsparcie dla następujących a) Windows 2012/2016/2019 oraz 8.x/10. b) Linux każda dystrybucja c) Urządzenia sieciowe Cisco, Check Point, F5 Networks, Juniper, Pulse Secure, Imperva, Palo Alto Networks, HP, Brocade d) Urządzenie DWDM Microsens Przez pozyskiwanie logów rozumie się: a) pobranie logów i zapisanie w bazie systemu SIEM, b) klasyfikacja zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.) c) normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source_ip itp.
2.2.	Dopuszcza się by zbudowanie obsługi ww. typów logów było w ramach wdrożenia. Możliwości oferowane przez system w ramach obsługi tworzonej w trakcie wdrożenia lub używania systemu nie mogą być mniejsze niż dla źródeł obsługiwanych natywnie przez produkt.
2.3.	System 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.
2.4.	Tworzenie mechanizmów:

	a) parsowania, b) integracji z nowymi protokołami w celu pobierania danych, c) normalizacji logów muszą być możliwe do wykonania przez Zamawiającego bez konieczności uzyskiwania jakichkolwiek akceptacji ze strony Producenta.
2.5.	System SIEM musi umożliwiać pobieranie logów i innych danych co najmniej następującymi protokołami: a) syslog UDP/TCP, b) trap SNMP, c) 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), d) pliki tekstowe, e) NetFlow v5 i v9, sFlow, jFlow, IPFIX, f) HTTP I HTTPS POST, g) RESTful API, h) parametry urządzeń pobierane z wykorzystaniem SNMP v2c/3, i) dane wydajnościowe Windows Performance Monitor, j) dowolne dane WMI, k) wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym, l) zmiany w zawartości plików i kluczy rejestrów. m) treść systemowych plików konfiguracyjnych Pobieranie danych z ww. protokołów musi być możliwe z wykorzystaniem jak i bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

2.6.	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: a) DHCP, b) DNS, c) HTTP, d) IMAP, e) SIP, f) SMB, g) SMTP, h) Oracle TNS, i) TDS, j) MySQL. Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze.

2.7.	Mechanizm opisany w punkcie 2.5 musi zapewniać funkcjonalność rozszyfrowywania sesji SSL/TLS w celu uzyskania możliwości zapisu informacji wymienionych powyżej również dla ruchu szyfrowanego.
2.8.	Mechanizm opisany w punkcie 2.5 musi zapewniać funkcjonalność wyodrębniania plików będących zawartością danych przesyłanych przez sieć dla co najmniej protokołów SMTP i http.
2.9.	Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http_user_agent) oraz opcjonalnie agregację danych dla dowolnie wybranych kluczy agregacji spośród pól dostępnych dla poszczególnych protokołów.
2.10.	System 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.
2.11.	Agent musi zapewniać możliwość szyfrowania i uwierzytelnia komunikacji z serwerem centralnym.
2.12.	Musi istnieć możliwość ograniczenia przepustowości wykorzystywanej przez agenta do transmisji danych.
2.13.	Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie
2.14.	System musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych.
2.15.	System musi umożliwiać analizowanie logów wielolinijkowych. Maksymalny wspierany rozmiar pojedynczego logu nie może być mniejszy niż 256kB.
3. Wymagania funkcjonalne - normalizacja danych	
3.1.	System 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.
3.2.	System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenia parserów. Nazwy pól powinny być określone strukturą XML
3.3.	System musi umożliwiać obsługę logów w formacie CEF bez konieczności tworzenia parserów. Nazwy pól powinny być określone strukturą CEF.
3.4.	System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenia parserów. Nazwy pól powinny być określone strukturą JSON.
3.5.	System 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.
3.6.	System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski” powinna tworzyć pole „user” o wartości „jkowalski”.
3.7.	Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach: a) Katalogi LDAP, b) Bazy danych, c) Bazy noSQL d) Hadoop. e) Dane geolokalizacyjne. f) Dane zawarte w logach (np. watchlisty budowane w na podstawie zdarzeń z różnych systemów). W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami, a wzbogacanie powinno odbywać w locie w trakcie odczytu danych z źródeł zewnętrznych.
3.8.	System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.
3.9.	System musi umożliwiać analizę logów 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).
3.10.	Dostarczona licencja nie może ograniczać w żaden sposób liczby podłączonych urządzeń ani zalogowanych lub utworzonych kont użytkowników.
4. Wymagania funkcjonalne - wyszukiwanie i przechowywanie danych	
4.1.	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.
4.2.	System SIEM musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów 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

4.3.	System 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.
4.4.	System SIEM musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS lub NFS lub iSCSI w celu przechowywania danych archiwalnych i danych COLD. Dane COLD muszą być dostępne w systemie w ten sam sposób jak dane dostępne on-line. Dopuszczalne jest by dane dostępne były z mniejszą wydajnością.
4.5.	System musi umożliwiać stosowanie macierzy obiektowych zgodnych z protokołem Amazon S3 jako alternatywę do mechanizmów opisanych w pkt 4.3 i 4.4.
4.6.	Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem.
5. Wymaganie funkcjonalne - narzędzia analityczne danych	
5.1.	Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól.
5.2.	System 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.
5.3.	System musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są w wielu formatach - minimum PDF, CSV, JPG.
5.4.	Zestaw funkcjonalności analitycznych systemu musi uwzględniać co najmniej następujące funkcje: a) Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego), b) Funkcje wykrywania anomalii danych liczbowych. System musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego.

	c) System musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze, d) Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól. Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%).
5.5.	System musi umożliwiać wykorzystanie w regułach, raportach i dashboardach mechanizmów uczenia maszynowego. System musi posiadać gotowe do użycia algorytmy ML co najmniej: • Detekcja anomalii: funkcja gęstości, współczynnik odstępstwa lokalnego (local outlier factor), OneClassSVM, modele Kelmana. • Klasyfikacji: BernoulliNB, GausianNB, klasyfikator drzewa decyzyjnego, regresja logistyczna, gradient boosting, perceptron wielowarstwowy, las losowy, • Klasteryzacji: BIRCH, DBSCAN, algorytm centroidów (K-means), spectral clustering. • Regresji: drzewo decyzyjne, regresja liniowa, las losowy, Lasso, RIDGE, • Analizy linii czasowy: ARIMA, równanie stanu. System musi zawierać wizualne narzędzia wspomagające parametryzację i testowanie
5.6.	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).
5.7.	System SIEM musi pozwalać na akceleracją 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.
5.8.	System SIEM musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem: a) Tabel, b) Lista zdarzeń, c) Wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy), d) Map, e) Map kolorowanych.
5.9.	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.

5.10.	Musi istnieć możliwość tworzenie 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).
5.11.	Musi istnieć możliwość definiowania akcji typu drill down związanych 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 drilldown. Musi istnieć możliwość przekazania parametrów metodami GET i POST.
5.12.	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.
5.13.	Dla warstwy analitycznej, System musi umożliwiać konfigurację klastrów wysokiej dostępności z równoważeniem obciążenia (klastry Active/Active). Musi istnieć możliwość konfiguracji dowolnej liczby węzłów klastra.
6. Wymagania funkcjonalne - analiza zdarzeń bezpieczeństwa	
6.1.	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)
6.2.	System SIEM musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danego systemu SIEM.
6.3.	Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości.
6.4.	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.
6.5.	Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.).
6.6.	System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej: a) Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych, b) Możliwość przypisania incydentu do osoby, c) Możliwość zmiany statusu i priorytetu incydentu, d) Możliwość tworzenia komentarzy,

	e) Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy. f) Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki. Możliwość raportowania wydajności obsługi incydentów.
6.7.	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.
6.8.	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.
6.9.	Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto.
6.10.	Musi istnieć możliwość prezentacji opisu zasobu w postaci serwera lub stacji roboczej obejmującego: nazwę, istotność, właściciela, funkcję, kontakt do administratora, 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.
6.11.	System SIEM musi klasyfikować ryzyko związane ze zdarzeniem z uwzględnieniem danych priorytetu hosta celu zdarzenia.
6.12.	System 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.
6.13.	System SIEM musi umożliwiać korzystanie z zewnętrznych subskrypcji tzw. wskaźników kompromitacji (ang. IOC). System musi wspierać dowolne subskrypcje zgodne z protokołami: a) http, b) ftp, c) TAXII, d) Facebook Threatconnect System musi również interpretować pliki w formacie CSV, STIX, OpenIOC, tekstowym interpretowanym z wykorzystaniem REGEX.
6.14.	System SIEM musi wspierać ww. wskaźniki wobec pól reprezentujących: a) Certyfikat X509, b) Adres email, c) Nazwa pliku, d) Suma kontrolna pliku, e) URL, f) Adres hosta lub domena, g) Adres IP,

	h) Nazwa procesu, i) Suma kontrolna procesu, j) Klucze rejestru, k) Nazwa usługi systemowej, l) Nazwa użytkownika. Musi istnieć możliwość rozbudowy funkcjonalności o nowe typy wskaźników samodzielnie przez administratora.
6.15.	Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach.
6.16.	System SIEM musi posiadać predefiniowane raporty/dashboardy związane z zarządzaniem bezpieczeństwem, co najmniej uwzględniające następujące zagadnienia: a) istotne zdarzenia bezpieczeństwa uwzględniające istotność zasobu informatycznego, b) aktywność złośliwego oprogramowania, c) aktywność użytkowników i wykorzystanie kont, d) zmiany w zawartości krytycznych obiektów systemowych, e) stan zainstalowanych poprawek/patchy dla oprogramowania systemowego, f) informacje o ruchu sieciowym, g) informacje dotyczące ataków sieciowych, h) wykorzystanie dostępu do Internetu przez użytkowników, i) wykryte podatności na podstawie raportów skanerów podatności, j) zmiany w konfiguracji urządzeń sieciowych, k) aktywność użytkowników (na podstawie tożsamości), l) raporty dotyczące obsługi incydentów przez operatorów systemu, m) raporty dotyczące wykrycia wskaźników kompromitacji.
6.17.	System SIEM musi pozwalać na definiowanie własnych i modyfikację raportów, zapytań i dashboardów dostarczonych przez producenta.
6.18.	Reguły dostarczone przez producenta muszą umożliwiać ich mapowanie do standardowych metodyk: MITRE ATT&CK, NIST Cyber Security Framework, Lockheed Martin Cyber Kill Chain.
6.19.	System musi umożliwiać podejmowanie automatycznych akcji lub alarmowania. Dostępne akcje muszą obejmować minimum: a) utworzenie incydentu w Systemie, b) wysłanie email, c) uruchomienie skryptu i przekazanie parametrów wywoławczych, d) integrację z systemami klasy service-desk, e) modyfikacja list kontrolnych. System musi zawierać API pozwalające na budowanie nowych akcji w tym przekazanie wybranych pól zdarzenia jako parametrów akcji.

7. Wymagania techniczne i bezpieczeństwa	
7.1.	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. Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi takich klient SSH lub RDP.
7.2.	System musi umożliwiać komunikację z SIEM za pomocą urządzeń mobilnych Apple IOS i Google Android, i pozwalać na integrację alarmów SIEM z powiadomieniami ww. urządzeń.
7.3.	System SIEM musi zostać dostarczony w konfiguracji zapewniającej odporność na awarię w zakresie komponentu przechowującego dane - klaster złożony z co najmniej 2 węzłów.
7.4.	System SIEM powinien 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 (np. Active Directory) i SAML 2.0.
7.5.	System nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników.
7.6.	System SIEM musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów - login/logoff, uruchamiane zapytania i zmiany konfiguracji systemu.
7.7.	System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healtcheck).
7.8.	System musi umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami systemu.
8. Wymagania inne	
8.1	Dostarczony system musi umożliwiać analizę 40 GB surowych danych dziennie.
8.2	Przekroczenie ww. parametrów nie może skutkować żadną utratą danych. System powinien informować o takim przekroczeniu w postaci alarmu i informacji w interfejsie użytkownika.
8.3	System musi zapewnić możliwość przechowywania danych (dane surowe i metadane) przez okres 1 roku od ich powstania.

8.4	Dostarczony system musi być objęty wsparciem producenta przez okres minimum 36 miesięcy.