PK XII BIA 0470.38.2021

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

*Rozbudowa posiadanych przez Zamawiającego licencji rozwiązania SIEM*

# Słownik pojęć i skrótów.

**POPD** – środowisko produkcyjne w Podstawowym Ośrodku Przetwarzania Danych,

**ZOPD** – środowisko produkcyjne w Zapasowym Ośrodku Przetwarzania Danych,

**OPD** – Ośrodek Przetwarzania Danych

**Oprogramowanie** – wartości niematerialne i prawne dostarczane w ramach przedmiotowego postępowania

**SOC** – ang. Security Operations Center

**ITS** – infrastruktura techniczno-systemowa

**Urządzenie/Sprzęt** – sprzęt teleinformatyczny (serwery, macierze itp.) dostarczany i/lub udostępniany przez Zamawiającego w ramach przedmiotowego postępowania.

**System -** posiadane przez Zamawiającego rozwiązanie Zarządzania Zdarzeniami (SIEM) którego rozbudowa jest przedmiotem postępowania.

# Ogólny Opis Przedmiotu Zamówienia

## Kontekst postepowania

Zamawiający planuje budowę centralnej, wspólnej dla wszystkich systemów informatycznych oraz infrastruktury informatycznej, platformy gromadzenia i korelacji logów w skali całej Prokuratury. Rozwiązanie obejmie swoim zasięgiem usługę katalogową, pocztę elektroniczną, urządzenia sieciowe, zdarzenia raportowane przez urządzenia fizyczne, logi generowane przez aplikacje biznesowe Zamawiającego oraz usługi działające na warstwie systemu operacyjnego. Na warstwie wdrożonego rozwiązania realizowana będzie korelacja zdarzeń z całości systemów teleinformatycznych Zamawiającego i jednostek podległych, scenariusze reakcji na incydenty obsługiwane przez strukturę SOC oraz obsługa śladu audytowego aplikacji biznesowych.

Zamawiający posiada rozwiązanie Splunk Enterprise Security w środowisku nieprodukcyjnym (licencja 5GB) oraz w środowisku produkcyjnym (licencja 200GB). W toku prowadzonych prac projektowych posiadana licencja okazała się niewystarczająca. W ramach przedmiotowego postępowania Zamawiający zamierza pozyskać licencję w środowisku produkcyjnym umożliwiającą przetwarzanie 2TB danych w oparciu o ilość procesorów oraz dla środowiska nieprodukcyjnego przenieść licencję z obecnego środowiska produkcyjnego.

## Przedmiot postępowania

Postępowanie przetargowe obejmuje:

1. Dostawę oprogramowania dla Środowiska Produkcyjnego.
2. Wykonanie Projektu Technicznego wdrożenia dla Środowiska Produkcyjnego i Środowiska Nieprodukcyjnego.
3. Instalacja i wdrożenie dostarczanego oprogramowania na udostępnionych zasobach zgodnie z Projektem Technicznym dla Środowiska Produkcyjnego i Środowiska Nieprodukcyjnego.
4. Przeprowadzenie testów dostarczanego oprogramowania wg zaakceptowanych przez Zamawiającego scenariuszy testów.
5. Opracowanie dokumentacji powykonawczej.
6. Opracowanie procedur utrzymania dostarczanego oprogramowania.
7. Szkolenia.
8. Gwarancja na dostarczone oprogramowanie.
9. Wsparcie techniczne.

# Opis stanu aktualnego

## Udostępniania infrastruktura

Zamawiający na potrzeby wdrożenia w środowisku produkcyjnym udostępni zasoby klastra VmWare umożliwiające uruchomienie maszyn o sumarycznych parametrach 400vCPU, 300GB RAM; 260TB przestrzeni dyskowej. Zamawiający nie przewiduje rozbudowy zasobów obecnego środowiska nieprodukcyjnego.

W przypadku większych wymagań dla optymalnego działania dostarczanego systemu SIEM, Wykonawca zobowiązany jest dostarczyć niezbędną infrastrukturę we własnym zakresie przy czym dostarczana infrastruktura musi w pełni współpracować z posiadanym i udostępnianym przez Zamawiającego rozwiązaniem opartym o serwery HP oraz macierze Dell EMC. Zamawiający udostępni szafę rack (42RU) na potrzeby dodatkowego wyposażenia. Zamawiający nie dostarcza licencji systemów operacyjnych na którym zostanie uruchomione rozwiązanie. Wykonawca musi przewidzieć odpowiednie licencje w ramach składanej oferty.

## Miejsce instalacji

Dostarczane oprogramowanie będzie instalowane i wdrażane w siedzibie Zamawiającego.

## Dostęp do sieci WAN-PROK

Zamawiający udostępnia zbiorcze łącze dostępowe do dedykowanej sieci WAN-PROK prokuratury o przepustowości 512Mbps.

## Dostęp do sieci Internet

Zamawiający udostępnia dostęp do Internetu poprzez 2 punkty styku wykreowane w zasobach operatora telekomunikacyjnego o przepustowości 2Gbps każdy.

## Zegar

W celu synchronizacji czasu Zamawiający udostępnia serwer czasu ELPROMA NTS-3000.

# System Zarządzania Zdarzeniami (SIEM)

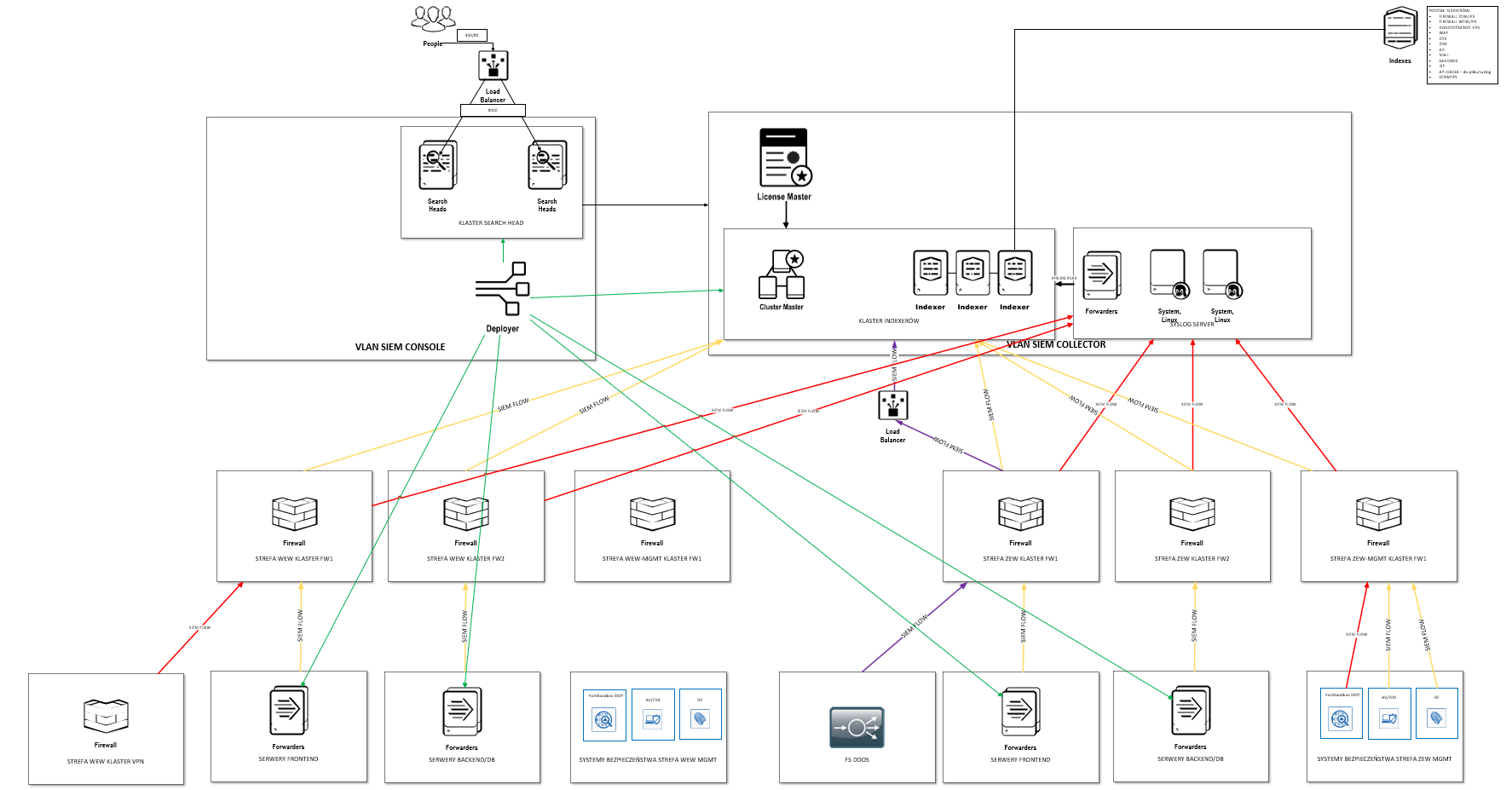
**Producent …………………..…………………………….……………….….\***

**Model …………………….………………………………………………\***

*\*- podać nazwę oferowanego oprogramowania/rozwiązania wraz z nazwą licencji umożliwiającą jednoznaczną identyfikację oferowanych funkcjonalności. W przypadku dostarczania elementów infrastruktury należy podać wszystkie nazwy, producentów oraz ukompletowanie dostarczanego Sprzętu.*

Przedmiotem zamówienia jest rozbudowa posiadanej przez Zamawiającego licencji Oprogramowania Splunk Enterprise Security do wersji umożliwiającej obsługę co najmniej dziennego przyrostu danych na poziomie 2 TB i 180-dniową retencję oraz przechowywanie danych w archiwum przez okres 18 miesięcy.

Obecnie wykorzystywany System Splunk Enterprise Security o wielkości licencji umożliwiającej przesyłanie danych wielkości 200GB dziennie został wdrożony w następującej architekturze.



Rys.1 Schemat infrastruktury SIEM Splunk

Zamawiający planuje uruchomienie Systemu w środowisku produkcyjnym z podłączonymi następującymi źródłami logów:

|  |  |
| --- | --- |
| **Rodzaj usługi lub urządzenia** | **Liczba urządzeń / nodów będących źródłami logów** |
| Active Directory (liczba serwerów DC) | 16 |
| Windows Server | 500 |
| Linux Server SUSE | 20 |
| Linux Server CENTOS / REDHAT | 40 |
| DNS | 16 |
| Systemy bezpieczeństwa np.: serwer systemu antywirusowego, firewall NGFW, inne | 450 |
| Centralny Firewall | 6 |
| Pomocniczy Firewall | 8 |
| IPS/IDS | 6 |
| VPN | 6 |
| WAF | 6 |
| System autoryzacji użytkowników sieci | 6 |
| Dedykowane aplikacje Zamawiającego | 1 |

Tabela 1 Źródła logów

Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania określone poniżej:

|  |  |
| --- | --- |
| ***Identyfikator wymagania*** | ***Opis wymagania*** |
| **SIEM-01** | **Platforma SIEM musi zapewnić mechanizmy nadzoru nad funkcjonowaniem systemów przetwarzania informacji w zakresie bezpieczeństwa informacji, ciągłości działania, wykrywania awarii, wykrywania anomalii i rozwiązywania problemów. Podstawowymi zadaniami dla systemu SIEM są m.in.:** |
| SIEM-01.01 | weryfikacja funkcjonowania zasad bezpieczeństwa i stosowanych środków kontrolnych, |
| SIEM-01.02 | zapewnienie mechanizmów monitorujących pracowników i innych użytkowników infrastruktury teleinformatycznej, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych. |
| SIEM-01.03 | podział obowiązków w zakresie monitorowania i rozliczania użytkowników uprzywilejowanych, |
| SIEM-01.04 | zarządzanie wykrywaniem, priorytetyzowaniem i rozwiązywaniem incydentów bezpieczenstwa, |
| SIEM-01.05 | zbieranie, zapisywania i przechowywanie logów na czas określony przez prawo i regulaminy wewnętrzne. Dane muszą być́ przechowywane w sposób zapewniający ochronę ich integralności, |
| SIEM-01.06 | korelacji informacji pochodzących z różnych źródeł w celu wykrycia zaawansowanych zagrożeń i/lub eliminacji fałszywych alarmów. |
| **SIEM-02** | **Wymagania ogólne** |
| SIEM-02.01 | System musi realizować funkcjonalność systemu zarządzania informacją i zdarzeniami bezpieczeństwa SIEM. |
| SIEM-02.02 | System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych, obejmujące:   1. analizę logów audytowych z aplikacji tworzonych na potrzeby Zamawiającego, 2. analizę logów pozwalających na weryfikację oraz wykrycie nieprawidłowego działania aplikacji tworzonych na potrzeby Zamawiającego, 3. mechanizmy pobierania danych, 4. raporty, dashboardy i formularze, 5. nowe funkcje analityczne, 6. nowe sposoby wizualizacji danych, 7. 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. |
| SIEM-02.03 | Architektura rozwiązania musi umożliwiać rozdzielenie na osobne serwery funkcji:   1. pobierania danych, 2. przechowywania, wyszukiwania i zarządzania bazą zebranych logów, 3. warstwy analitycznej i interfejsu użytkownika. |
| SIEM-02.04 | System musi zostać dostarczony w konfiguracji wysokiej dostępności eliminującej wystąpienie Single Point of Failure. |
| SIEM-02.05 | Zaoferowane rozwiązanie nie może posiadać ograniczeń w postaci ilości urządzeń z których pobierane są logi jak również ilości zdarzeń na sekundę (EPS). |
| SIEM-02.06 | Licencja systemu musi dopuszczać dowolne kształtowanie architektury systemu, w szczególności stosowanie dowolnej liczby komponentów poszczególnych funkcji opisanych w wymaganiu SIEM-02.03 |
| SIEM-02.07 | Oferowane rozwiązanie musi być rozwiązaniem komercyjnym, posiadającym wsparcie techniczne producenta. Nie dopuszcza się rozwiązań open source. |
| SIEM-02.08 | Oferowane funkcjonalności muszą mieć pokrycie w oficjalnie dostępnej dokumentacji technicznej producenta, którą dostawca udostępni na żądanie Zamawiającego wraz ze wskazaniem punktów odnoszących się do danej funkcjonalności wymaganej w OPZ. |
| SIEM-02.09 | 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. |
| SIEM-02.10 | Oferowane rozwiązanie musi posiadać wsparcie techniczne na terenie Polski. |
| SIEM-02.11 | Rozwiązanie powinno 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. |
| **SIEM-03** | **Wymagania funkcjonalne – pozyskiwanie danych** |
| SIEM-03.01 | Zaoferowane rozwiązanie musi umożliwiać pobieranie logów / danych zapisanych w plikach (dziennikach systemowych / aplikacyjnych) jak również w postaci komunikatów przechwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów:   1. Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (np. syslog). 2. Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay. 3. Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog. 4. Wykonywanie przez zaoferowane rozwiązania zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC. 5. Windows Management Infrastructure (WMI). |
| SIEM-03.02 | System musi umożliwiać zaprojektowanie i wdrożenie przesyłania, parsowania, korelowania i przechowywania logów i innych danych z co najmniej z następujących źródeł:   1. Systemy bezpieczeństwa: Check Point, Palo Alto, Juniper SSG, McAfee ePO, Trend Micro Deep Security, Pulse Connect Secure, Fidelis, Fudo, CyberArk, 2. Firewalle WAF: F5 Networks, Imperva, Fortinet, 3. Urządzenia Fortinet: firewalle, FortiSandbox, FortiMail 4. Urządzenia CISCO: przełączniki, routery, firewalle, 5. Systemu operacyjne: Red Hat, Microsoft Windows, 6. Usługi serwerowe: DNS, DHCP, WWW (Apache, IIS), 7. Bazy danych: Oracle, SQL Server, MySQL, Postgres, 8. Systemy wirtualizacji: Vmware vSphere, Red Hat Virtualization, 9. Logi Windows Events (Logi Application, Security, System I inne), 10. Logi z ruchu sieciowego poprzez Netflow, 11. Logi z systemu kontroli dostępu. |
| SIEM-03.03 | Rozwiązanie musi pozwalać na analizę standardowych logów infrastrukturalnych generowanych przez systemy operacyjne, firewalle, urządzenia sieciowe (przełączniki, routery, loadbalancery, itd.) systemy bezpieczeństwa IPS/IDS/Application & URL Filtering / Anti-Bot, WAF, IDM, DAM, itd. |
| SIEM-03.04 | Rozwiązanie 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. |
| SIEM-03.05 | System musi umożliwiać pobieranie logów co najmniej następującymi protokołami:   1. syslog UDP/TCP, 2. trap SNMP, 3. logi i informacje przechowywane w bazach danych co najmniej 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. WMI, 6. NetFlow v5 i v9, sFlow, jFlow, IPFIX,   Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów. |
| SIEM-03.06 | System 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 co najmniej następujących protokołów:   1. DHCP, 2. DNS, 3. HTTP, 4. IMAP, 5. SMTP.   Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera. |
| SIEM-03.07 | 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. |
| SIEM-03.08 | Agent musi zapewniać możliwość szyfrowania i uwierzytelnia komunikacji z serwerem centralnym. |
| SIEM-03.09 | System musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych. |
| SIEM-03.10 | Oprócz źródeł wymienionych wyżej system musi umożliwiać pobieranie informacji z wykorzystaniem poniższych mechanizmów:   1. parametry życiowe urządzeń pobierane z wykorzystaniem SNMP v2c/3, 2. wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym, 3. pliki tekstowe na zdalnych serwerach. |
| SIEM-03.11 | Rozwiązanie musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię. |
| SIEM-03.12 | Rozwiązanie powinno pozwalać na analizę niestandardowych logów wygenerowanych przez aplikacje utworzone na potrzeby Zamawiającego. |
| **SIEM-04** | **Wymagania funkcjonalne – normalizacja danych** |
| SIEM-04.01 | 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. |
| SIEM-04.02 | System musi umożliwiać obsługę logów w formacie CEF |
| SIEM-04.03 | System musi umożliwiać obsługę logów w formacje JSON |
| SIEM-04.04 | System musi umożliwiać obsługę logów w formacje CSV |
| SIEM-04.05 | System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski” powinno tworzyć pole „user” o wartości „jkowalski”. |
| SIEM-04.06 | 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.   W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami a wzbogacanie musi odbywać w locie w trakcie odczytu danych ze źródeł zewnętrznych. |
| SIEM-04.07 | System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót. |
| SIEM-04.08 | System 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 (UTF8 lub UTF16). |
| SIEM-04.09 | Licencja nie może ograniczać w żaden sposób liczby podłączonych urządzeń. |
| **SIEM-05** | **Wymagania funkcjonalne – wyszukiwanie i przechowywanie danych** |
| SIEM-05.01 | System musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie surowej (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. |
| SIEM-05.02 | System musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów klastra w celu spełnienia wymagań dot. wydajności lub dostępności |
| SIEM-05.03 | System musi samodzielnie zarządzać retencją danych. |
| SIEM-05.04 | Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. |
| SIEM-05.05 | Rozwiązanie powinno umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę dla co najmniej 400TB danych. |
| SIEM-05.06 | Rozwiązanie musi wspierać mechanizm planowanego przenoszenia danych na pamięci masowe niższego poziomu na podstawie czasu lub okresu. |
| SIEM-05.07 | 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, a nie w trakcie zapisu. |
| SIEM-05.08 | System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS/NFS w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line. |
| SIEM-05.09 | System musi zapewnić kontrolę dostępu na poziomie Role Based Access Control w granulacji określonej na poziomie wartości poszczególnych, identyfikowanych danych. |
| **SIEM-06** | **Wymaganie funkcjonalne – narzędzia analityczne danych** |
| SIEM-06.01 | 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. |
| SIEM-06.02 | System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach, jeśli są dostępne. System musi uwzględniać przy prezentacji wyniku możliwość pozyskiwania logów z urządzeń skonfigurowanych w innych strefach czasowych. |
| SIEM-06.03 | Rozwiązanie musi umożliwiać wyszukiwanie zdarzeń́ w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX) lub gotowych wzorców wyboru np: adres IP źródłowy/docelowy, port, protokół. |
| SIEM-06.04 | 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%). |
| SIEM-06.05 | System 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). |
| SIEM-06.06 | System musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem:   1. Tabel, 2. Listy zdarzeń, 3. Wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy), 4. Map, 5. Map kolorowanych,   Tworzenie wyżej wymienionych komponentów wizualizacji musi odbywać się bezpośrednio na poziomie zapytania. |
| SIEM-06.07 | 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. |
| SIEM-06.08 | Musi istnieć możliwość definiowania akcji typu „drill down” związanych 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. |
| SIEM-06.09 | Rozwiązanie musi umożliwiać przeglądanie (w jednej konsoli systemu) logów pobieranych/dostarczanych do Systemu w celu uniknięcia konieczności logowania się̨ do każdego monitorowanego systemu osobno, w celu sprawdzenia statusu połączenia (przepuszczone, zablokowane). Filtrowanie w czasie rzeczywistym musi dopuszczać́ wyszukiwanie informacji za pomocą̨ wyrażeń́ regularnych (REGEX) lub gotowych wzorców np: adres IP źródłowy/docelowy, port, protokół. |
| SIEM-06.10 | Rozwiązanie musi umożliwiać wydajną pracę użytkownika przeglądającego zdarzenia i generującego raporty oraz samego rozwiązania, w szczególności parsowania danych, których wielkość dochodzi do 2 TB dziennie. |
| **SIEM-07** | **Wymagania funkcjonalne – analiza zdarzeń bezpieczeństwa** |
| SIEM-07.01 | System 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). |
| SIEM-07.02 | Rozwiązanie musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne dla zdarzeń mają służyć do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych. |
| SIEM-07.03 | System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI jak i języka zapytań charakterystycznego dla danego systemu SIEM. |
| SIEM-07.04 | Musi istnieć możliwość zastosowania reguł korelacyjnych dla danych historycznych w celu wykrycia podobnych zdarzeń w przeszłości. |
| SIEM-07.05 | System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania. Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie. |
| SIEM-07.06 | Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.). |
| SIEM-07.07 | System 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. |
| SIEM-07.08 | System 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. |
| SIEM-07.09 | Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto. |
| SIEM-07.10 | System musi klasyfikować ryzyko związane ze zdarzeniami z uwzględnieniem danych priorytetu hosta celu zdarzenia. |
| SIEM-07.11 | 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. |
| SIEM-07.12 | System musi umożliwiać korzystanie z zewnętrznych subskrypcji tzw. wskaźników kompromitacji (ang. IOC). |
| SIEM-07.13 | System musi wspierać ww. wskaźniki wobec pól reprezentujących co najmniej:   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.   Musi istnieć możliwość rozbudowy funkcjonalności o nowe typy wskaźników samodzielnie przez administratora. |
| SIEM-07.14 | Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach. |
| SIEM-07.15 | Rozwiązanie musi posiadać predefiniowane widoki dedykowane dla specjalistów odpowiedzialnych za poszczególne domeny bezpieczeństwa, np.:   1. wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu; 2. wykrywanie i obsługa podatności; 3. analiza ruchu sieciowego; 4. analiza oraz śledzenie wykorzystywanych portów i protokołów; 5. analiza oraz śledzenie aktualizacji oprogramowania w ramach organizacji; 6. analiza i śledzenie uprawnień dostępu. |
| SIEM-07.16 | System musi pozwalać na definiowanie własnych i modyfikację raportów, zapytań i dashboardów dostarczonych przez producenta. |
| SIEM-07.17 | System musi umożliwiać podejmowanie automatycznych akcji lub alarmowanie. Dostępne akcje muszą obejmować:   1. utworzenie incydentu, 2. wysłanie email, 3. uruchomienie skryptu i przekazanie parametrów wywoławczych, 4. integrację z systemami klasy service-desk, 5. modyfikacja list kontrolnych, |
| SIEM-07.18 | Systemie musi mieć możliwość́ tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej, a także automatycznego, cyklicznego wysyłania raportów poprzez e-mail w postaci PDF. |
| **SIEM-08** | **Wymagania techniczne i bezpieczeństwa** |
| SIEM-08.01 | Komunikacja użytkownika z Systemem musi odbywać się przy użyciu przeglądarki internetowej. 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. |
| SIEM-08.02 | System nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników. |
| SIEM-08.03 | System musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji Systemu. |
| SIEM-08.04 | Rozwiązanie musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healtcheck). |
| SIEM-08.05 | Rozwiązanie musi umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami Systemu. |
| SIEM-08.06 | Reguły korelacji muszą być́ tworzone i zarządzane w interfejsie systemu, bez potrzeby użycia dodatkowych narzędzi firm trzecich. |
| SIEM-08.07 | Rozwiązanie musi umożliwiać́ wykrywanie sytuacji niestandardowej, niezgodnej z poprzednio zarejestrowanym wzorcem (np. w celu wykrycia ataku DoS, wykrycia wewnętrznego ruchu sieciowego który wcześniej nie występował, uruchomienia nowej niewystępującej wcześniej aplikacji, pojawienia się̨ nowego użytkownika itp). |
| SIEM-08.08 | System musi wspierać́ pracę użytkowników o rożnych rolach i w następujących obszarach:   1. Analiza zdarzeń́ w obszarze bezpieczeństwa teleinformatycznego. 2. Analiza pracy systemów informatycznych w zakresie wydajności i awarii systemów/urządzeń́ teleinformatycznych. 3. Analiza pracy aplikacji wdrażanych/tworzonych na potrzeby Zamawiającego |
| SIEM-08.09 | Rozwiązanie musi umożliwiać́ odseparowanie środowiska pracy użytkowników o rożnych rolach. |
| SIEM-08.10 | System musi zawierać́ minimum 300 stworzonych i dostarczonych przez producenta oferowanego rozwiązania wbudowanych reguł korelacyjnych działających na danych ze źródeł logów i pakietów skonfigurowanych w trakcie wdrożenia. |
| SIEM-08.11 | Rozwiązanie musi umożliwiać́ tworzenie alertów/powiadomień́ po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę̨ korelacyjną. |
| SIEM-08.12 | Wdrożone rozwiązanie musi być́ odporne na ataki sieciowe. W tym celu niezbędne jest zabezpieczenie/hardening rozwiązania obejmujący usunięcie niepotrzebnego/nieużywanego oprogramowania systemowego, kont użytkowników, wyłączenie zbędnych usług oraz włączenie filtrowania ruchu IP. |

# Dostawa sprzętu i oprogramowania

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOSSPRZ-01 | Wykonawca opracuje szczegółową specyfikację dostaw realizowanych przez Wykonawcę w ramach Umowy – Plan Dostaw. |
| DOSSPRZ-02 | Plan dostawy musi zawierać szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego. |
| DOSSPRZ-03 | Plan dostaw musi zawierać procedurę odbioru jakościowego. |
| DOSSPRZ-04 | Plan dostaw musi zawierać procedurę zmian terminów w trakcie realizacji dostaw. |
| DOSSPRZ-05 | Plan dostaw musi zawierać procedurę obsługi uszkodzeń sprzętu w trakcie dostawy. |
| DOSSPRZ-06 | Plan dostaw musi zawierać specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostawy. |
| DOSSPRZ-07 | Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego. |
| DOSSPRZ-08 | Wykonawca dostarczy sprzęt w godzinach od 7:00 do 16:00 w dni robocze od poniedziałku do piątku. |
| DOSSPRZ-09 | Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| DOSSPRZ-10 | Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| DOSSPRZ-11 | Wykonawca jest zobowiązany do wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania. Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie i środki transportu umożliwiające wykonanie tych prac. |
| DOSSPRZ-12 | Dostarczana ITS musi być zgodna z prawem obowiązującym podmioty publiczne. W szczególności wymagana jest zgodność z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych |
| DOSSPRZ-13 | Wykonawca musi dostarczyć niewyspecyfikowane elementy ITS, które są niezbędne do prawidłowego funkcjonowania wyspecyfikowanych elementów ITS. |
| DOSSPRZ-14 | Wykonawca musi zapewnić, że wszystkie dostarczane produkty (dotyczy to zarówno sprzętu jak i oprogramowania) są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca. |
| DOSSPRZ-15 | Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) niezbędny do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10% , 50 Hz. |
| DOSSPRZ-16 | Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, z załączonymi kartami gwarancyjnymi i instrukcjami obsługi w języku polskim (przy czym Zamawiający wymaga, aby urządzenia były rozpakowane i uruchomione wyłącznie przez Wykonawcę, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu). |
| DOSSPRZ-17 | Wykonawca dostarczy wszystkie licencje wymagane do działania funkcjonalności opisanych w OPZ. |
| DOSSPRZ-18 | Wykonawca dostarczy wszystkie klucze licencyjne wymagane do instalacji i działania dostarczanego Oprogramowania. |
| DOSSPRZ-19 | Wykonawca dostarczy dokładny opis zasad licencjonowania dostarczanego Oprogramowania. |
| DOSSPRZ-20 | W przypadku, gdy licencja oprogramowania objęta jest opłatą okresowej opieki wówczas Wykonawca poda wszystkie dane umożliwiające przedłużenie czasu opieki przez Zamawiającego. |

# Projekt Techniczny wdrożenia dla Środowiska Produkcyjnego i Środowiska Nieprodukcyjnego (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PRO-01 | Wykonawca opracuje Projekt Techniczny wdrożenia dla Środowiska Produkcyjnego i Środowiska Nieprodukcyjnego umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym. |
| PRO-02 | Wykonawca opracuje projekt rozmieszczenia szaf „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń (w przypadku dostarczenia dodatkowych elementów infrastruktury ITS).  Zamawiający dostarczy dokumentację projektową, będącą w jego posiadaniu i istotną dla opracowania projektu technicznego montażu i instalacji ITS, w terminie 3 dni roboczych od dnia podpisania umowy. |
| PRO-03 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby udostępniane przez Zamawiającego oraz ewentualnie dostarczone w ramach niniejszego postępowania. |
| PRO-04 | Projekt Techniczny wdrożenia dla Środowiska Produkcyjnego i Środowiska Nieprodukcyjnego musi zawierać minimum:   1. Wykaz wykorzystanego sprzętu i licencji oprogramowania. 2. Przyjęte nazewnictwo elementów infrastruktury. 3. Plan ustawienia szaf w pomieszczeniach serwerowni *(w przypadku dostawy dodatkowych elementów ITS).* 4. Plan rozmieszczenia sprzętu w szafach *(w przypadku dostawy dodatkowych elementów ITS).* 5. Wymagania dotyczące zasilania i klimatyzacji oraz wagi poszczególnych szaf rack *(w przypadku dostawy dodatkowych elementów ITS).* 6. Projekt zarządzania infrastrukturą w serwerowni *(w przypadku dostawy dodatkowych elementów ITS)*. 7. Projekt konfiguracji infrastruktury wirtualizacji *(w przypadku dostawy dodatkowych elementów ITS)*. 8. Projekt konfiguracji zasobów dyskowych *(w przypadku dostawy dodatkowych elementów ITS)*. 9. Projekt instalacji systemów operacyjnych na dostarczonych/udostępnianych serwerach wirtualnych z uwzględnieniem wygenerowania certyfikatów na potrzeby bezpiecznej komunikacji pomiędzy komponentami Systemu oraz użytkowników/operatorów/administratorów Systemu. 10. Projekt migracji obecnego rozwiązania (w środowisku produkcyjnym i środowisku nieprodukcyjnym) Zamawiającego i zgromadzonych w nich danych oraz reguł korelacji do rozwiązania wdrażanego w ramach przedmiotowego postępowania. Migracja rozwiązań agentowych służących do przekierowania logów do aktualnie wykorzystywanego systemu dla wszystkich obsługiwanych serwerów. 11. Projekt konfiguracji infrastruktury sieci LAN (matrix ruchu sieciowego w celu uruchomienia zbierania logów ze wskazanych źródeł) oraz dostęp ze wskazanych stacji administracyjnych. 12. Projekt przekierowania logów do systemu z warstwy ITS oraz warstwy systemów operacyjnych i aplikacji dedykowanych w środowisku Zamawiającego. 13. Projekt uruchomienia dedykowanych dashboardów opartych o zdefiniowane źródła logów dla personelu SOC *(Zamawiający prowadzi inne postępowanie przetargowe związane z pozyskaniem usługi SOC)*. 14. Projekt integracji dostarczanego rozwiązania z istniejącą infrastrukturą oraz systemami operacyjnymi serwerów Zamawiającego w celu wyzwalania określonych akcji będących reakcjami na określone typy zdarzeń uzgodnionych na etapie przygotowywania Projektu Technicznego. 15. Projekt uruchomienia predefiniowanych w dostarczanym rozwiązaniu oraz dodatkowych (do 60 sztuk dodatkowych reguł korelacji) uzgodnionych z Zamawiającym reguł korelacji z uwzględnieniem potrzeb aplikacji dedykowanych Zamawiającego. 16. Projekt integracji z posiadanym przez Zamawiającego rozwiązaniem PIM/PAM. |

# Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| MONTS-01 | Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty ITS (Oprogramowania oraz Sprzętu w przypadku dostawy dodatkowych elementów ITS) w POPD zgodnie z opracowanym szczegółowym projektem technicznym. |
| MONTS-02 | Wykonawca dostarczy licencje Oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację Systemu Zarządzania Zdarzeniami (SIEM) zgodnie z wymaganiami OPZ. |
| MONTS-03 | Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, kable Ethernet kat. 6e, bezpieczniki, gniazda zasilające, moduły PDU do szaf rack, organizery okablowania itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń zarówno dostarczanych w ramach przedmiotowego postępowania. W ramach prac Wykonawcy leży podłączenie wszystkich oferowanych rozwiązań do sieci LAN i SAN Zamawiającego - w przypadku dostawy dodatkowych elementów ITS |
| MONTS-04 | Wykonawca dokona montażu całości sprzętu w szafach RACK w pomieszczeniach POPD i ZOPD zgodnie z opracowanym szczegółowym projektem technicznym - w przypadku dostawy dodatkowych elementów ITS. |
| MONTS-05 | Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zapewniający redundancję - w przypadku dostawy dodatkowych elementów ITS. |
| MONTS-06 | Wykonawca wykona odpowiednie przyłącza elektryczne od rozdzielni elektrycznych w budynku do paneli PDU w szafach rack. Każde urządzenie posiadające redundantne zasilacze zostanie podłączone do dwóch niezależnych torów zasilania elektrycznego. W każdej szafie rack pozostanie wolnych co najmniej 5 gniazd elektrycznych z każdego toru zasilania - w przypadku dostawy dodatkowych elementów ITS. |
| MONTS-07 | Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania - w przypadku dostawy dodatkowych elementów ITS. |
| MONTS-08 | Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp. - w przypadku dostawy dodatkowych elementów ITS. |
| MONTS-09 | Wykonawca dokona aktualizacji oprogramowania układowego (firmware, BIOS) wszystkich urządzeń ITS do najnowszych stabilnych wersji - w przypadku dostawy dodatkowych elementów ITS. |
| MONTS-10 | Wszystkie nośniki danych dostarczane wraz z urządzeniami pozostają w siedzibie Zamawiającego. Wykonawca dostarczy na płytach CD/DVD komplet sterowników systemowych i niezbędne oprogramowanie narzędziowe i fabryczne - w przypadku dostawy dodatkowych elementów ITS. |

# Konfiguracja środowisk zgodnie z Projektami Technicznymi (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PRACE-01 | Wykonawca przeprowadzi proces aktualizacji Oprogramowania oraz oprogramowania sprzętowego dostarczonych Urządzeń (w przypadku dostawy dodatkowych elementów ITS) do najnowszych dostępnych stabilnych, rekomendowanych przez producenta wersji oprogramowania. |
| PRACE-02 | Wykonawca zainstaluje i skonfiguruje Oprogramowanie zgodnie z opracowanymi Projektami Technicznymi oraz wszystkie dostarczane i/lub udostępnianie przez Zamawiającego Urządzenia/Infrastrukturę na potrzeby wdrożenia Systemu Zarządzania Zdarzeniami (SIEM) zgodnie z wymaganiami OPZ. |

# Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| TESTY-01 | Wykonawca przeprowadzi testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów. |
| TESTY-02 | Wykonawca opracuje dla każdego rodzaju testów Plan Testów który musi być zaakceptowany przez Zamawiającego. |
| TESTY-03 | Testami zostanie objęta realizacja i poprawność reguł korelacji zaimplementowanych w dostarczanym rozwiązaniu oraz utworzonych na etapie realizacji projektu. |
| TESTY-04 | Wykonawca przed przeprowadzeniem testów przeprowadzi instruktaż dla testerów Zamawiającego. |

# Wymagania na opracowanie dokumentacji powykonawczej (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOKPOW-01 | Wykonawca opracuje szczegółową dokumentację powykonawczą zawierającą dokładny opis architektury wdrożenia, instalacji i konfiguracji zainstalowanych komponentów ITS oraz Oprogramowania. |
| DOKPOW-02 | Dokumentacja powykonawcza będzie zawierała szczegółowe opisy zastosowanych rozwiązań wraz ze wskazaniem miejsca, w którym zawarto opis spełnienia każdego z wymagań. |
| DOKPOW-03 | Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word 2016) a także w wersji PortableDocument Format (zgodny z ISO 32000-1:2008). Na żądanie Zamawiającego lub jeśli wynika to z Umowy Wykonawca dostarczy dokument w wersji drukowanej (wydruk kolorowy) i/lub w wersji stanowiącej skan Dokumentu. |
| DOKPOW-04 | Wykonawca opracuje „Dokumentację administratora”. |
| DOKPOW-05 | Dokumentacja administratora powinna zawierać co najmniej:   1. Procedury administracyjne, 2. Procedury instalacji i konfiguracji, 3. Procedury bieżących działań administracyjnych, 4. Procedury okresowych/planowanych działań administracyjnych, 5. Procedury aktualizacji Oprogramowania oraz jego poszczególnych komponentów, 6. Procedury włączenia i wyłączenia Oprogramowania oraz sprzętu na którym jest zainstalowane. |
| DOKPOW-06 | Dokumentacja administracyjna oraz użytkowa musi być spójna z dokumentacją powykonawczą. |
| DOKPOW-07 | W ramach dokumentacji powykonawczej Wykonawca opracuje Politykę Bezpieczeństwa wdrożonego rozwiązania wraz z analizą ryzyka oraz analizą BIA. |

# Wymagania na opracowanie procedur utrzymania (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PROCUT-01 | Wykonawca opracuje szczegółowe procedury eksploatacyjne wdrożonego Oprogramowania.  Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania, dołożenie dodatkowego komponentu zbierającego logi lub przetwarzającego logi, realizacja dodatkowej reguły korelacyjnej, wyzwalanie akcji związanych z obsługą zdarzenia itp.. Procedury muszą obejmować wszystkie czynności, jakie należy wykonać w celu realizacji danego działania. |
| PROCUT-02 | Procedury zostaną przetestowane przez Zamawiającego przy udziale inżyniera Wykonawcy. Procedury będą na bieżąco poprawiane przez Wykonawcę w ramach wdrożenia. |
| PROCUT-03 | Wykonawca opracuje i uzgodni katalog usług powstałych w ramach Projektu do implementacji w posiadanym przez Zamawiającego rozwiązaniu ITSM Atmosfera. |
| PROCUT-04 | Wykonawca opracuje procedury dla administratorów lokalnych umożliwiające korzystanie z produktów Projektu oraz procedury dla pracowników zewnętrznych dokonujących obsługi incydentów. |

# Wymagania na szkolenia i warsztaty

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SZKOL-01 | Wykonawca zapewni szkolenia i warsztaty z zakresu funkcjonalności dostarczanego Oprogramowania. Przewidywana ilość uczestników warsztatów to **maksymalnie 25 osób** wskazanych przez Zamawiającego. |
| SZKOL-02 | Wykonawca opracuje plan warsztatów oraz plan szkoleń. Warsztaty z zakresu wdrażanego rozwiązania **będą trwać 4 dni robocze** i będą miały charakter tzw. „bootcamp”. W ramach warsztatów nastąpi przegląd wdrożonych reguł korelacyjnych oraz scenariuszy reakcji na zdarzenia, zagadnienia związane z zaawansowaną administracją rozwiązaniem, modelowanie danych, tworzenie własnych aplikacji w środowisku Splunk, zarządzanie bezpieczeństwem w systemie Splunk (użytkownicy i role) tworzenie, obsługa, archiwizacja i parametryzacja indeksów, metody integracji źródeł danych, obsługa incydentów.  Zapewnienie odpowiedniego środowiska warsztatowego leży po stronie Wykonawcy. |
| SZKOL-03 | W zakresie warsztatów zadaniem Wykonawcy jest zapewnienie:   * 1. bazy noclegowej – dla organizatorów i uczestników      1. Obiekt nie może być w trakcie prac remontowych w czasie trwania warsztatów.      2. Wykonawca zapewnia wszystkie miejsca noclegowe w sposób zapewniający samodzielny pobyt w pokoju (Zamawiający dopuszcza zakwaterowanie samodzielne jednego uczestnika w pokoju dwuosobowym)      3. Każdy z pokoi noclegowych z łazienką, TV, łącze internetowe (Wi-Fi) posiadających otwierane okna lub działającą klimatyzację.      4. Obiekt co najmniej \*\*\* (trzy gwiazdki), w rozumieniu przepisów § 2 ust. 2 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz. U. z 2006 r., Nr 22, poz. 169 ze zm.). Na każde żądanie Zamawiającego Wykonawca obowiązany jest okazać kopię decyzji właściwego Marszałka Województwa o nadaniu kategorii hoteli na podstawie art. 38 ust.1 i art. 42 ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2014 r., poz. 196 ze zm.),      5. Na terenie obiektu lub w bezpośrednim jego sąsiedztwie powinien znajdować się bezpłatny parking.      6. Obiekt powyżej trzech pięter powinien zostać wyposażony w windę      7. Warsztaty, nocleg oraz wyżywienie powinny odbywać się na terenie tego samego obiektu.   2. odrębnych sal szkoleniowych dla każdej, równolegle szkolonej grupy. Każda z sal wykładowych przeznaczona jest maksymalnie dla 25 osób ze stanowiskiem dla wykładowców oraz miejscem na sprzęt multimedialny. Wszystkie sale szkoleniowe muszą być klimatyzowane i posiadać dostęp do światła dziennego oraz zapewniać komfortowe warunki do prowadzenia w nich szkoleń/warsztatów (tj. odpowiednie oświetlenie, odpowiednia temperatura).   3. każda sala szkoleniowa musi być wyposażona w rzutnik multimedialny, ekran do wyświetlania prezentacji, tablicę do pisania lub flipchart z arkuszami papieru i pisakami, skaner, stację zarządzającą i stanowiska szkoleniowe dla każdej ze szkolonych osób, wyposażone w stację roboczą i zestaw 2-monitorowy. Wykonawca zapewni w miejscu przeprowadzania szkoleń/warsztatów urządzenia sieciowe celem połączenia ze środowiskiem warsztatowym zorganizowanym po stronie Wykonawcy. Czas wykorzystania sal pierwszego dnia od godz. 12.00 do 20.00, pozostałe dni od godz. 8.00 do 19.00. Zamawiający dopuszcza wykorzystanie komputerów przenośnych pracowników Zamawiającego w celu połączenia ze środowiskiem laboratoryjnym.   4. noclegów dla uczestników szkolenia/warsztatów w pokojach jednoosobowych z łazienkami lub dwuosobowych z łazienkami do samodzielnego wykorzystania **(Wykonawca ma obowiązek zapewnić nocleg każdej osobie w odrębnym pokoju).** Czas trwania doby hotelowej od godz. 11.00 pierwszego dnia szkolenia do godz. 16.00 ostatniego dnia szkolenia. Miejsca noclegowe muszą znajdować się na terenie tego samego obiektu, co sale wykładowe.   5. Wyżywienia dla uczestników szkolenia składającego się z:  1. śniadania podawanego w formie bufetu, 2. obiadu w formie bufetu, 3. kolacji w formie bufetu, 4. przerw kawowych (całodziennych, uzupełniany serwis konferencyjny), składający się:   - świeżo parzoną gorącą kawę naturalną oraz herbatę w torebkach  - cytrynę, cukier, mleko,  - sok owocowy 100%,  - butelkowana woda mineralna gazowana i niegazowana,  - co najmniej 3 rodzaje kruchych ciasteczek.   1. Posiłki, które będą podawane podczas szkoleń/warsztatów muszą być przygotowywane na terenie obiektu w którym odbywa się szkolenie. Wyklucza się ich dowożenie.    1. W zakresie wyżywienia Wykonawca zobowiązany jest do: 2. Terminowego przygotowania posiłków zgodnie z ustalonym harmonogramem. 3. Zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowywaniu posiłków. 4. Przygotowywania posiłków zgodnie z zasadami racjonalnego żywienia, urozmaiconych (każdego dnia szkolenia inne menu), przygotowywanych ze świeżych produktów z ważnymi terminami przydatności do spożycia. 5. Wyżywienie dla trenerów oraz innych osób zaangażowanych w obsługę szkolenia/warsztatów Wykonawca zapewnia na swój koszt. |
| SZKOL-04 | Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 10 dni przed rozpoczęciem warsztatów, odpowiednich materiałów szkoleniowych, włączając w to materiały dla uczestników. Zamawiający zastrzega sobie prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych. |
| SZKOL-05 | Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy szkoleń i warsztatów. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia. |
| SZKOL-06 | Program szkoleń i warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu szkoleń i warsztatów. Zamawiający zastrzega prawo do korekty programu szkoleń / warsztatów w uzgodnionym zakresie. |
| SZKOL-07 | Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru warsztatu wraz z dołączonymi załącznikami tj. oryginalną listą obecności, harmonogramem i programem warsztatu. |
| SZKOL-08 | Szkolenia muszą być autoryzowane przez producenta produktu, którego dotyczą. Szkolenia muszą być prowadzone w języku polskim. Osoba/osoby prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne i doświadczenie dydaktyczne do prowadzenia szkoleń. |
| SZKOL-09 | Szkolenia muszą być przeprowadzone w ośrodku szkoleniowym na terenie Warszawy. |
| SZKOL-10 | Każdy uczestnik szkolenia/warsztatu otrzyma certyfikat jego ukończenia. |
| SZKOL-11 | Szkolenia zostaną zrealizowane w postaci voucher-ów na autoryzowane szkolenia z zakresu wdrażanego Oprogramowania Systemu Zarządzania Zdarzeniami (SIEM). Wykonawca dostarczy **15 voucherów na szkolenia z zakresu podstawowej oraz zaawansowanej administracji rozwiązaniem oraz 10 voucherów z zakresu analizy danych.** Vouchery będą ważne co najmniej 24 miesiące od dnia podpisania Protokołu Odbioru Końcowego. |
| SZKOL-12 | W przypadku zaprzestania przez dany ośrodek szkoleniowy prowadzenia szkoleń z danego tematu musi istnieć możliwość zamiany vouchera na szkolenie równoważne. |
| SZKOL-13 | W ramach warsztatów i szkoleń uczestnicy otrzymają komplet materiałów szkoleniowych w wersji papierowej oraz elektronicznej obejmujących swoim zakresem całe szkolenie. Wszystkie materiały szkoleniowe muszą być w języku polskim lub angielskim. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych. |
| SZKOL-14 | Wykonawca zapewni prowadzenie szkoleń/warsztatów przez wykwalifikowaną kadrę posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia oraz profesjonalny przebieg i organizację. |
| SZKOL-15 | Wykonawca dostarczy wszystkie materiały pomocnicze niezbędne do przeprowadzenia warsztatów i szkoleń, jak np. materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć. |
| SZKOL-16 | Szkolenia powinny odbywać się w formie wykładów i warsztatów praktycznych w proporcji obejmującej co najmniej 75 % warsztatów. |
| SZKOL-17 | Szkolenia i warsztaty odbywać się będą w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin dziennie. Cykl szkolenia nie może być dzielony między tygodniami |
| SZKOL-18 | Wykonawca zapewni ciepły posiłek, w formie zestawu obiadowego (zupa, drugie danie, napój), dla każdego uczestnika szkolenia, we wszystkie dni szkolenia, podczas przerwy obiadowej. |

# Wymagania na serwis gwarancyjny

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| GWAR-SER-01 | Zgłoszenia awarii następować będzie w trybie 24/7/365 i musi być dokonywane w postaci: zgłoszenia telefonicznego, z wykorzystaniem serwisu www lub za pomocą poczty elektronicznej, wszystkie wymienione kanały komunikacji muszą być świadczone w języku polskim. |
| GWAR-SER-02 | W ramach gwarancji Wykonawca zapewni następujące usługi:   1. zdalne wsparcie techniczne (możliwość zgłaszania problemów w trybie 24x7), 2. wsparcie w miejscu instalacji (w trybie 24x7) 3. pozostawienie uszkodzonych dysków u Zamawiającego, 4. części zamienne oraz ich instalację, 5. uaktualnienia oraz instalację uaktualnień Oprogramowania nie rzadziej niż raz na 180 dni w siedzibie Zamawiającego, jeżeli takie uaktualnienia są rekomendowane przez Producenta Sprzętu i/lub Oprogramowania (dla krytycznych uaktualnień bezpieczeństwa Wykonawca dokona aktualizacji niezwłocznie). 6. dostęp do internetowych narzędzi serwisowych. |
| GWAR-SER-03 | Wykonawca jest zobowiązany do niezwłocznego potwierdzenia przyjęcia zgłoszenia na adres poczty elektronicznej: ………@pk.gov.pl, podany przez Zamawiającego lub telefonicznie - na numer podany podczas rejestracji zgłoszenia (czas reakcji). W przypadku braku potwierdzenia po upływie 4 godzin od zgłoszenia awarii przez Zamawiającego, Zamawiający wdroży procedurę eskalacji zgłoszenia. |
| GWAR-SER-4 | Zamawiający musi mieć możliwość bezpośredniego zgłaszania awarii do producenta sprzętu (w języku polskim) oraz samodzielnej aktualizacji oprogramowania (szczegółowa instrukcja instalacji/aktualizacji zostanie dostarczona najpóźniej w dniu podpisania Protokołu odbioru). W okresie obowiązywania umowy samodzielna aktualizacja oprogramowania będzie realizowana każdorazowo po uzgodnieniu z Wykonawcą |
| GWAR-SER-5 | W okresie obowiązywania serwisu gwarancyjnego wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Uszkodzone dyski podlegające gwarancji stanowią własność Zamawiającego i pozostają u Zamawiającego, nie podlegają zwrotowi w ramach usługi gwarancyjnej |
| GWAR-SER-6 | Usługi gwarancyjne muszą być realizowane przez autoryzowany serwis producenta albo przez Wykonawcę na terenie Polski dla każdego urządzenia i oprogramowania na warunkach określonych w Opisie Przedmiotu Zamówienia |
| GWAR-SER-7 | Wykonawca zobowiązany jest zapewnić dostęp Zamawiającego do aktualizacji oprogramowania standardowego oraz dostarczyć opis procedur pozyskiwania informacji o dostępności aktualizacji oraz sposobu instalacji aktualizacji. |
| GWAR-SER-8 | **Wykonawca zapewni asystę techniczną, zgodnie z potrzebami Zamawiającego, przez minimum jednego inżyniera w danym obszarze związanym z przedmiotem zamówienia w okresie 36 miesięcy, licząc od dnia podpisania Protokołu Odbioru Umowy, w wymiarze do 400 roboczogodzin (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny).** |
| GWAR-SER-9 | Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym usługami w ramach udzielonej gwarancji. |
| GWAR-SER-10 | Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności modyfikacji wdrożonych rozwiązań oraz wsparciu w zakresie utrzymania. |
| GWAR-SER-11 | Świadczenie usługi asysty technicznej inżyniera jest jednostronnym uprawnieniem Zamawiającego. Nie skorzystanie przez Zamawiającego z tej usługi lub niewykorzystanie wszystkich przewidzianych w Umowie roboczogodzin nie rodzi po stronie Wykonawcy żadnych roszczeń w stosunku do Zamawiającego. |