Opis przedmiotu zamówienia

Wykonawca dostarczy, wdroży i przeszkoli pracowników Wydziału IT z rozwiązania do zbierania logów składającego się z licencjonowanego systemu wraz z przynajmniej rocznym wsparciem producenta, serwera o określonych poniżej parametrach w pkt 2. z oficjalnej polskiej dystrybucji wraz z gwarancją producenta sprzętu oraz licencji na program do zarzadzania macierzą o określonych poniżej parametrach w pkt 3.
W ramach wdrożenia wykonawca uruchomi i skonfiguruje system do zbierania logów oraz zainstaluje serwer w siedzibie Wielkopolskiego Zarządu Dróg Wojewódzkich w Poznaniu, bezprzerwowo i bez zakłócenia pracy innych działających systemów produkcyjnych.

Wymagania ogólne dla całego przedmiotu zamówienia

1) System do zbierania logów powinien zbierać logi z systemów opisanych poniżej oraz zapisywać je na dostarczonym przez Dostawcę serwerze i przechowywać na systemie do zarzadzania macierzą.
2) System powinien być oparty na komercyjnym licencjonowaniu producenta systemu.
3) System powinien posiadać wsparcie producenta.
4) System będzie zainstalowany na środowisku wirtualnym zamawiającego.
5) Serwer musi być fabrycznie nowy, pochodzić z autoryzowanego kanału sprzedaży producenta i w przypadku urządzeń reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się produktów: odnawianych, demonstracyjnych lub powystawowych.
6) Nie dopuszcza się produktów posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
7) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
8) Serwer musi być dostarczony Zamawiającemu w oryginalnym opakowaniu producenta.
9) Do urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.
10) Możliwość sprawdzenia statusu gwarancji oraz konfiguracji oferowanego serwera na stronie producenta po podaniu nr seryjnego serwera.

1. System do zbierania logów

1) Ogólna charakterystyka

a) System musi wykorzystywać nierelacyjną, rozproszoną bazę danych opartą o system Elasticsearch w wersji minimum 7;
b) System musi pracować w oparciu o architekturę Linux;
c) System musi mieć możliwość centralnego zbierania i zarządzania logami;
d) System musi działać w trybie zbliżonym do rzeczywistego;
e) System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu;

f) Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu;
g) System musi zapewniać efektywną obsługę co najmniej 4000 EPS lub 150 GB danych dziennie;
h) System musi zapewniać retencję danych w okresie minimum 90 dni;
i) System musi zapewniać możliwość jednoczesnej pracy dla co najmniej 10 użytkowników;
j) System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska;
k) Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja;
l) Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności powinno odbywać się bez konieczności restartu działającego systemu;
m) System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji;
n) System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie po przywróceniu pełnej sprawności systemu;
o) Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2;
p) System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer;
q) Interfejs musi posiadać angielską lub polską wersję językową;
r) System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinien spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1);
s) System musi zbierać logi ze źródeł danych Zamawiającego wymienionych poniżej:
   - Urządzenia sieciowe firm takich jak: Cisco, Hillstone, Juniper, MikroTik, Ubiquiti.
   - Systemów operacyjnych takich jak: Windows 10, Windows Server 2012 lub nowszy, Ubuntu, Debian, Centos, NetApp Ontap, VMware (vCentrer i ESXi), oraz systemy wirtualne zarządzane przez VMware.
   - Serwerów firm takich jak: Dell EMC, HPE, Supermicro, Lenovo, Qnap, Synology.
   - Inne urządzenia do monitorowania takie jak: UPS, Listwa PDU, Urządzenia monitorujące warunki środowiskowe, Kamery IP.

2) Dostęp do systemu

a) Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem;
b) Autoryzacja do systemu musi być zintegrowana z:
   - Microsoft Active Directory Domain Services,
   - LDAP,
   - Radius;
c) Hasła dostępowe Microsoft Active Directory Domain Services, muszą być przechowywane w postaci zaszyfrowanej;
d) System musi wspierać mechanizm logowania typu Single Sign On;
e) System musi umożliwiać zarzadzanie czasem automatycznego wygasania sesji użytkowników;
f) System musi posiadać dedykowany widok zarządzania użytkownikami i rolami;

g) System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika;
h) System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień;
i) System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych;
j) System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.

3) Przyjmowanie, identyfikacja i wizualizacja danych

a) System musi pozwalać na tworzenie parserów z poziomu GUI;
b) System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning;
c) System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów;
d) System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP;
e) Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach;
f) System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
g) System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
   - Syslog,
   - WEF,
   - Flat file,
   - Event log,
   - WMI,
   - SNMP trap,
   - XML,
   - Netflow,
   - JSON,
   - CSV,
   - Email,

   Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
h) System musi wykorzystywać do przyjmowania zdarzeń mechanizmy agentowe jak i bezagentowe;
i) System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.

j) Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera;
k) System musi posiadać predefiniowany zestaw parserów zdarzeń;
l) System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania;
m) System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach;
n) Proces parsowania musi umożliwiać wzbogacanie treści obieranych wiadomości poprzez matematyczne operacje wykonywane na innych polach;
o) Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa;
p) System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych;
q) System powinien pozwalać na rozpoznanie formatów czasu i daty i normalizowanie ich do jednego wspólnego formatu.

4) Reguły korelacyjne, alerty i obsługa incydentów

a) Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów;
b) System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym;
c) System musi posiadać bazę minimum 500 predefiniowanych reguł korelacyjnych;
d) System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących;
e) System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
   - Wykrycia dowolnej treści w logach,
   - Wykrycia wystąpienia wartości pola na wybranej liście,
   - Wykrycia niewystępowania wartości pola na wybranej liście,
   - Wykrycia zmiany jednego z kilku pól,
   - Wykrycia zdarzeń występujących z zadaną częstotliwością,
   - Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
   - Wykrycia zaniku wiadomości,
   - Wykrycia nowej wartości pola w zadanym okresie czasu,
f) System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów;
g) Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API;
h) System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym;
i) System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych;

j) System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. NetFlow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności;
k) System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta;
l) System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu;
m) System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook;
n) System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów;
o) Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT;
p) System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących;
q) Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat);
r) System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu;
s) System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi;
t) System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1;
u) System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark;
v) System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST;
w) System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów;
x) System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows ;
y) System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP;
z) System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule;
ź) Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.

4) Raportowanie

a) System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie;
b) Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu;
c) System musi generować raporty do formatów minimum PDF, JPEG, CSV z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.

5) Wymagania niefunkcjonalne

a) System powinien być zaoferowany w formie licencji wraz ze wsparciem producenta;
b) Oferowany system musi być rozwijany oraz musi być zapewniona możliwość zakupu wsparcia producenta przez co najmniej 5 lat od daty zakupu.
c) Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów;
d) Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów;
e) Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu;
f) System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych;
g) Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów;
h) Support producenta musi być świadczony w formule minimum 8/5;
i) Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz w siedzibie Zamawiającego;
j) Wykonawca wraz z licencją produkcyjną zobligowany jest dostarczyć licencję na potrzeby środowiska testowego, która umożliwi przetwarzanie minimum 1000 EPS;
k) Licencja testowa musi być objęta wsparciem producenta ta takich samych zasadach, jak licencja produkcyjna.

2. Serwer o następującej minimalnej konfiguracji:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji minimum 12 dysków 3.5" Hot-Plug oraz zainstalowanymi 12 ramkami do dysków 3.5'' typu Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor ośmio-rdzeniowe min. 2.1GHz klasy x86 dedykowany do pracy z zaoferowanym serwerem osiągające wynik w testach SPECrate2017_int_base nie gorszy niż 72.6 wynik musi być dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	Pamięci o parametrach 128GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling.
Gniazda PCI	Minimum trzy sloty generacji 3
Interfejsy sieciowe/FC/SAS	Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT dodatkowo zainstalowane: Broadcom 57416 dwuportowa karta sieciowa Mezzanine LOM 10GbE SFP+ wraz z 2 przewodami
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD**.** zainstalowane dyski: 6 x 4TB 7.2K SATA 6Gbps Hot-Plug Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID 1. możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w dwa nośniki typu flash o pojemności min. 32GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, tylne: min. 1x VGA, min. 1x port szeregowy RS232, min. 2x USB 3.0, min. 2 porty RJ45 port wewnętrzny: min. 1x USB 3.0.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne
Zasilacze	2 Redundantne zasilacze typu Hot-Plug maksymalnie 750W każdy z dedykowanymi przewodami zasilającymi.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. wbudowany moduł TPM 2.0
System operacyjny	Zainstalowany darmowy wirtualizator np. ESXi wraz z systemem do zarzadzania macierzą
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika możliwość podmontowania zdalnych wirtualnych napędów

	wirtualną konsolę z dostępem do myszy, klawiatury wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer integracja z Active Directory możliwość obsługi przez ośmiu administratorów jednocześnie wsparcie dla automatycznej rejestracji DNS wsparcie dla LLDP wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej możliwość podłączenia lokalnego poprzez złącze RS-232. możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. monitorowanie zużycia dysków SSD możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, automatyczne zgłaszanie alertów do centrum serwisowego producenta automatyczne update firmware dla wszystkich komponentów serwera możliwość przywrócenia poprzednich wersji firmware możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych integracja z Active Directory możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram

	szczegółowy opis wykrytych systemów oraz ich komponentów możliwość eksportu raportu do CSV, HTML, XLS, PDF możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. grupowanie urządzeń w oparciu o kryteria użytkownika tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach szybki podgląd stanu środowiska podsumowanie stanu dla każdego urządzenia szczegółowy status urządzenia/elementu/komponentu generowanie alertów przy zmianie stanu urządzenia. filtry raportów umożliwiające podgląd najważniejszych zdarzeń integracja z service desk producenta dostarczonej platformy sprzętowej możliwość przejęcia zdalnego pulpitu możliwość podmontowania wirtualnego napędu kreator umożliwiający dostosowanie akcji dla wybranych alertów możliwość importu plików MIB przesyłanie alertów ,,as-is'' do innych konsol firm trzecich możliwość definiowania ról administratorów możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

	wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. zdalne uruchamianie diagnostyki serwera. dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V
Oprogramowanie do zarządzania	Serwer musi być kompatybilny i zarządzany przez posiadane oprogramowanie Zamawiającego do zarządzania serwerami OpenManage Server Administrator (OMSA)
Certyfikaty	serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. serwer musi posiadać deklaracja CE. oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2 x64, Microsoft Windows Server 2016, Microsoft Windows Server 2019.
Warunki gwarancji	Min. trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

3. Licencja do zarządzania macierzą

W ramach dostawy Wykonawca dostarczy Zamawiającemu licencję na oprogramowanie do magazynowania danych i zarzadzania macierzą na pojemność przynajmniej 16 TB na okres przynajmniej 12 pełnych miesięcy, który będzie wspierał obecne oprogramowanie Zamawiającego typu SDS Netapp Ontap Select w zakresie:
- zapewnia obsługę wielu protokołów min. CIFS, NFS, iSCSI,
- integruje się ściśle z usługami ActiveDirectory i umożliwia zarządzanie uprawnieniami,
- umożliwia tworzenie szybkich kopii migawkowych z możliwością odtwarzanie w skali czasu,
- umożliwia rozbudowę o funkcje wysokiej dostępności (synchroniczna i asynchroniczna replikacja),

- klaster łączący w sobie technologię klastra macierzy z synchronicznym mirroringiem – przejęcie funkcjonalności przez inny węzeł bez przerwy w pracy systemu (przejęcie pełnej funkcjonalności np. konfiguracja sieci, zapewnienie dostępu do tych samych danych),
- wirtualizujące zasoby dyskowe (DAS) serwera fizycznego,
- szyfrowanie danych które wykorzystuje 256-bitowe klucze AES,
- może użyć funkcjonalności takich jak: deduplikacja, kompresja i kompakcja,
- zarządzanie oprogramowaniem przez protokół SSH lub przeglądarkę internetową zgodną z HTML5

4. Usługa wdrożenia i uruchomienia systemu do zbierania logów

W ramach wdrożenia Zamawiający oczekuje:

a) Opracowanie harmonogramu wdrożenia systemu SIEM;
b) Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu technicznego wdrożenia;
c) Przeprowadzenie instalacji i konfiguracji systemu SIEM;
d) Podłączenie do systemu wskazanych przez Zamawiającego w punkcie 1. 1) s) OPZ źródeł danych;
e) Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem;
f) Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia;
g) Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do zidentyfikowanych źródeł danych.
h) Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.
i) Proponowane scenariusze będą przedłożone Zamawiającemu do akceptacji.

5. Szkolenie pracowników Wydziału IT

a) Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem SIEM dla 4 pracowników Zamawiającego w wymiarze 2 dni roboczych (min. 16h robocze);
b) Grupa szkoleniowa będzie miała nie więcej niż 4 słuchaczy;
c) Szkolenie odbędzie się w siedzibie Zamawiającego;
d) Szkolenie musi być prowadzone w języku polskim;
e) Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim;
f) Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.