Ministerstwo Rozwoju i Technologii **Warszawa, 16.09.2025 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na zakup systemu Zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM - Security Information and Event Management) oraz systemu Orkiestracja, Automatyzacja i Reagowanie na Incydenty Bezpieczeństwa (SOAR - Security Orchestration, Automation, and Response) wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego zamówienia do wszczęcia postępowania przetargowego na zakup systemów SIEM oraz SOAR.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia, jest zakup systemu Zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM - Security Information and Event Management) dalej SIEM oraz systemu Orkiestracja, Automatyzacja i Reagowanie na Incydenty Bezpieczeństwa (SOAR - Security Orchestration, Automation, and Response) dalej SOAR wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego.

Zakres zamówienia obejmuje w szczególności:

1. dostawę i konfigurację elementów infrastruktury przeznaczonych do uruchomienia systemu SIEM wraz ze wsparciem technicznym na okres wskazany w formularzu ofertowym, na który składają się:
   a) dedykowana hybrydowa macierz dyskowa klasy Enterprise oparta o dyski SSD i HDD wraz z wsparciem producenta na okres 36 miesięcy;
   b) klaster wirtualizacji składający się z serwerów fizycznych wraz z oprogramowaniem Vmware wraz ze wsparciem producenta na okres 36 miesięcy;
   c) klaster przełączników Ethernet w celu połączenia klastra serwerów fizycznych z siecią Zamawiającego wraz z wsparciem producenta na okres 36 miesięcy;
   d) klaster przełączników SAN w celu połączenia klastra serwerów z dostarczoną macierzą dyskową wraz z wsparciem producenta na okres 36 miesięcy;
2. dostawę licencji dla systemu Zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM - Security Information and Event Management) wraz ze wsparciem na okres określony w formularzu ofertowym (na potrzeby oszacowania wartości zamówienia Zamawiający wymaga wyceny dla dwóch wariantów czasowych na okres 24 i 36 miesięcy);
   a. WARIANT 1 – Licencja nieograniczona w czasie typu MULTITENANT (z możliwością obsługi wielu klientów) wraz z wsparciem, (na potrzeby oszacowania wartości zamówienia Zamawiający wymaga wyceny dla dwóch wariantów czasowych);
   b. WARIANT 2 - Licencja nieograniczona w czasie bez MULTITENANT (Licencja która obsługuję tylko jedną organizację).
   c. Jeżeli w celu realizacji opisanych funkcjonalności wymagane są subskrypcje na dodatkowe usługi np. dostęp do baz IOC to należy je również dostarczyć na okres 24 lub 36 miesięcy (na potrzeby oszacowania wartości zamówienia Zamawiający wymaga wyceny dla dwóch wariantów czasowych). Wszystkie subskrypcje muszą zostać dokładnie wyszczególnione w formularzu technicznym.
3. dostawę licencji w formie subskrypcji dla systemu Orkiestracja, Automatyzacja i Reagowanie na Incydenty Bezpieczeństwa (SOAR - Security Orchestration, Automation, and Response) na okres określony w formularzu ofertowym (na potrzeby oszacowania wartości zamówienia Zamawiający wymaga wyceny dla dwóch wariantów czasowych na okres 24 i 36 miesięcy):
   a. WARIANT 1 – Licencja typu MULTITENANT (Z możliwością obsługi wielu klientów)
   b. WARIANT 2 - Licencja bez MULTITENANT (Licencja która obsługuję tylko jedną organizację.
4. wdrożenie dostarczonych systemów SIEM oraz SOAR, w tym:
   a) instalację dostarczonych urządzeń i subskrypcji oprogramowania,
   b) konfigurację, uruchomienie i testowanie, w tym dodatkowych elementów,
   c) wykonanie dokumentacji technicznej i eksploatacyjnej,
   d) przeprowadzenie instruktażu dla administratorów Systemu.
5. usługi asysty technicznej dla wdrożonego Systemu, świadczone na podstawie dodatkowych zleceń Zamawiającego w tym:
   a) integracje nowych technologii;
   b) rozbudowa systemu o nowe komponenty;

c) podłączanie nowych źródeł danych.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 60 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).**

Wykonawcy zainteresowani realizacją zamówienia w celach uzyskania szczegółów związanych ze szczegółami technicznymi w „Załączniku do wymiarowania systemu SIEM" oraz w „Załączniku do wymiarowania systemu SOAR", w terminie składania ofert mogą wystąpić w drodze kontaktu mailowego na adres ofertyIT@mrit.gov.pl o udostępnienie niniejszych załączników.

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. W ramach przedmiotu zamówienia zostanie zrealizowana dostawa systemu Zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM - Security Information and Event Management) oraz systemu Orkiestracja, Automatyzacja i Reagowanie na Incydenty Bezpieczeństwa (SOAR - Security Orchestration, Automation, and Response) wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego.
2. Dostawa nastąpi do siedziby Zamawiającego, przy Placu Trzech Krzyży 3/5 w Warszawie.
3. W ramach realizacji przedmiotu zamówienia zostaną dostarczone urządzenia wraz z niezbędnymi elementami do tych urządzeń i licencjami oprogramowania składającego się na zaoferowany System Zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM - Security Information and Event Management) oraz system Orkiestracja, Automatyzacja i Reagowanie na Incydenty Bezpieczeństwa (SOAR - Security Orchestration, Automation, and Response)
4. Wszystkie elementy dostarczone z każdym z urządzeń stanowiących przedmiot zamówienia, będą pochodziły od producenta dostarczanego urządzenia.. Stosowane elementy muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej
5. Zaoferowane urządzenia muszą być fabrycznie nowe przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz.U. z 2004 r., nr 204, poz. 2087 j.t. z późn. zm.) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych" (ang. Refurbished). Zaoferowane urządzenia, oprogramowanie sterujące połączeniami oraz aplikacje zarządzające muszą pochodzić od tego samego producenta co dostarczane urządzenia/licencje. Zamawiający wymaga, aby dostarczone Systemy SIEM i SOAR pochodziły z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.
6. Zamawiający wymaga, aby zaoferowane urządzenia/oprogramowanie były dostępne i serwisowane przez Producenta oraz nie były przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

IV. MINIMALNE WYMAGANIA TECHNICZNE MACIERZY DYSKOWEJ

1. Macierz dyskowa będzie przechowywać dane typu log. (Większy wolumen danych, mniej IOPS)
2. Macierz musi obsługiwać dyski SSD oraz HDD.
3. Macierz musi zostać zbudowana z wykorzystaniem dysków SSD o pojemności nie mniejszej niż 3.84 TB każdy.
4. Macierz musi zostać zbudowana z wykorzystaniem dysków HDD o pojemności nie mniejszej niż 16TB i prędkości obrotowej dysku 7.2K RPM każdy.
5. Macierz musi być wyposażona w minimum **40TB** przestrzeni **SSD** użytecznej do zapisu (Bez zachowania funkcjonalności kompresji oraz deduplikacji)
6. Macierz musi być wyposażona w minimum **200 TB** Przestrzeni **HDD** użytecznej do zapisu (Bez zachowania funkcjonalności kompresji oraz deduplikacji)
7. Macierz musi zapewniać wysoką dostępność danych z użyciem RAID (RAID 6, RAID DP – Double Parity) lub ich odpowiedników jeżeli producent stosuje inne techniki redundancji danych.
8. Macierz musi zapewnić mechanizm automatycznej wymiany dysku w przypadku uszkodzenia Hot-Spare. Konfiguracja macierzy musi zapewniać minimum 2 dyski w trybie Hot-Spare dla każdej grupy dyskowej.

9. Macierz musi zapewniać obsługę udostępniania przestrzeni za pomocą protokołów FC (Fibre Channel).
10. Macierz musi być wyposażona w redundatne kontrolery dysków N+1 lub N+N z obsługą funkcji Hot-Swap w formie active-active lub active-passive.
11. Każdy kontroler musi być wyposażony w minimum 2 interfejsy SFP+ 16Gb dla protokołu FC wraz z certyfikowanymi przez producenta wkładkami.
12. Każdy kontroler musi być wyposażony w minimum 1 interfejs RJ45 dedykowany do zarządzania macierzą.
13. Macierz musi zapewnić natywną możliwość replikacji wolumenów na drugą macierz w trybie asynchronicznym.
14. Macierz musi być posiadać możliwość konfiguracji za pomocą dedykowanych administratorowi interfejsów GUI (Dostępnego przez przeglądarkę i protokół HTTPS) oraz CLI (Dostępnego przez protokół SSH)
15. Macierz musi posiadać wsparcie dla systemów operacyjnych VMware vSphere oraz Microsoft Windows Server potwierdzone przez producenta tych systemów.
16. Macierz musi posiadać możliwość monitorowania poszczególnych komponentów za pomocą systemu Zabbix z użyciem protokołów SNMP lub HTTP.
17. Macierz musi posiadać możliwość wysyłania logów zdarzeń za pomocą protokołu SYSLOG.
18. Macierz musi posiadać możliwość integracji autentykacji z Active Directory za pomocą protokołu LDAP.
19. Zamawiający wymaga dostarczenia macierzy wraz ze wsparciem producenta na okres wskazany w formularzu ofertowym.
20. Uszkodzone dyski pozostają własnością Zamawiającego.
21. Macierz musi być przystosowana do montażu w szafie rack 19”.
22. Każdy kontroler musi posiadać co najmniej 24GB pamięci RAM.
23. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest monitorowanie bieżących parametrów pracy macierzy.
24. Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych.
25. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie typu Thin Provisioning.
26. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych.
27. Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
28. Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny z wykorzystaniem protokołu FC i IP. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.
29. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary wolumenów logicznych) z poziomu interfejsu administratora.
30. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
31. Macierz musi wspierać podłączenie następujących systemów operacyjnych dla protokołu FC: Windows Server 2022, Red Hat 9.x, VMware 8.x, SLES 15.
32. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.
33. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.
34. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
35. Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy.
36. Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii.
37.

V. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE KLASTRA PRZEŁĄCZNIKÓW ETHERNET

Obecnie Zamawiający posiada infrastrukturę sieciową opartą o cztery rodzaje przełączników: Cisco Catalyst 3650, 9200, 9500. Sprzęt będący przedmiotem niniejszego zamówienia musi

być kompatybilny z posiadaną przez Zamawiającego infrastrukturą. Zaoferowany sprzęt nie może powodować zmniejszenia funkcjonalności posiadanych przełączników sieciowych.
Dostarczony klaster (2 sztuki) przełączników Ethernet musi spełniać następujące wymagania:

1. Zaoferowane przełączniki sieciowe oraz oprogramowanie muszą pochodzić od tego samego producenta.
2. Typ i liczba portów w każdym z przełączników - 24-porty 1/10/25G SFP/SFP+/SFP28 i 4 porty 40G/100G QSFP+
3. Porty SFP/SFP+/SFP28 możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
   a) Porty SFP+/ SFP28 - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax 10/25G-CSR, 10/25G-LR
   b) Porty QSFP+ - wkładki 40Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, twinax, wkładki 100Gigabit Ethernet w tym 100G-SR4, 100G-LR4, 100G-SM-SR, 100G-ER4L
   c) Z każdym przełącznikiem musi zostać dostarczony zestaw kabli i modułów optycznych pochodzących od Producenta przełącznika:
      a. Kabel typu 25Gb AOC SFP28, min. 3m – min. 10 szt.
      b. Kabel typu 100 Gb AOC QSFP28 min. 1m – min. 1 szt.
      c. Moduł optyczny typu 25Gb SFP-25G-SR – min. 10 szt.
      d. Moduł optyczny typu 10Gb SFP-10G-SR – min. 10 szt.
      e. Kabel typu 100Gb AOC QSFP28 min. 10m – min. 1 szt.
4. Zasilanie i chłodzenie
   a) Redundantne i wymienne moduły wentylatorów
   b) Zainstalowany dodatkowo zasilacz redundantny AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
5. Parametry wydajnościowe:
   a) Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
   b) Bufor pakietów – 32MB
   c) Pamięć DRAM – 16GB
   d) Pamięć flash – 16GB
   e) Obsługa:
      a. 4.000 sieci VLAN
      b. 82.000 adresów MAC
      c. 200.000 tras IPv4
      d. 200.000 tras IPv6
6. Obsługa protokołu NTP
7. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
8. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   a) IEEE 802.1w Rapid Spanning Tree
   b) Per-VLAN Rapid Spanning Tree (PVRST+)
   c) IEEE 802.1s Multi-Instance Spanning Tree
   d) Obsługa 128 instancji protokołu STP
9. Obsługa protokołu LLDP i LLDP-MED.
10. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
11. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
12. Możliwość uruchomienia funkcji serwera DHCP
13. Mechanizmy związane z bezpieczeństwem sieci:
    a) Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    b) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    c) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    d) Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    e) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    f) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X

g) Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
h) Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
i) 27.000 wpisów dla list kontroli dostępu (Security ACE)
j) Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
k) Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
l) Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
m) Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
n) Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
o) Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch i switch-host) kluczami o długości 128-bitów (gcm-aes-128)
p) Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)
q) Funkcja Private VLAN

14. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
    a) Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
    b) Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
    c) Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.
15. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a) Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b) Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
    c) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    d) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    e) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)
    f) Kontrola sztormów dla ruchu broadcast/multicast/unicast
    g) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
16. Obsługa protokołów routingu:
    a) Routing statyczny dla IPv4 i IPv6
    b) Routing dynamiczny – RIP, OSPF, EIGRP (Zamawiający wykorzystuje dynamiczny protokół routingu EIGRP w infrastrukturze sieciowej)
    c) Policy-based routing (PBR)
    d) Obsługa protokołu redundancji bramy (VRRP)
17. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
18. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
19. Zarządzanie:
    a) Port konsoli,
    b) Dedykowany port Ethernet do zarządzania out-of-band,
    c) Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

d) Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
e) Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
f) Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
g) Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
h) Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

20. Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU.
21. Przełącznik musi posiadać funkcjonalność połączenia dwóch przełączników w stos (z wykorzystaniem standardowych modułów optycznych/twinax) celem stworzenia pojedynczego logicznego przełącznika z zapewnieniem następujących funkcjonalności:
    a) Zarządzanie poprzez jeden adres IP,
    b) Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
    c) Możliwość aktualizacji oprogramowania w trakcie pracy stosu (ISSU – In Service Software Upgrade),
22. Wsparcie dla protokołu LISP zgodnie z RFC 6830
23. Obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN)
24. Obsługa zaawansowanych protokołów routingu
    a) IS-IS i BGP dla IPv4 i IPv6
    b) Routing multicastów - PIM-SM, PIM-SSM
    c) Multicast Source Discovery Protocol (MSDP)
    d) VRF-Lite
25. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256)
26. Możliwość enkapsulacji ruchu w pakiety VXLAN
27. Wsparcie dla IEEE 1588v2 (PTP – Precision Time Protocol)
28. Wsparcie dla IEEE 802.1BA (AVB – Audio Video Bridging)
29. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 98.000 strumieni
30. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
31. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku
32. Funkcjonalność bramy dla usług mDNS
33. Wbudowany analizator pakietów
34. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN)
35. Przełącznik musi posiadać deklaracja CE lub równoważną.
36. Przełącznik musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.

VI. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE KLASTRA PRZEŁĄCZNIKÓW SAN

Dostarczony klaster (2 sztuki) przełączników SAN musi spełniać następujące wymagania:

1. Przełącznik Fibre Channel musi mieć wysokość maksymalnie 1U (jednostka wysokości szafy montażowej) i zapewniać techniczną możliwość montażu w szafie 19"
2. Przełącznik FC musi być wykonany w technologii Brocade FC 16 Gb/s oraz 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.
    a) W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji
    b) W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji
    c) Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. Oversubskrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s.
    d) Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end.
3. Ilość i rodzaj portów Fibre Channel:

a) Przełącznik Fibre Channel musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzone 8 wkładkami SFP+, wielomodowymi, krótkodystansowymi, ze złączem LC o prędkości 32 Gbit każda.
b) Wszystkie dostarczone wkładki muszą być oryginalne, tj. dostarczane przez producenta oferowanego przełącznika, lub certyfikowane przez producenta oferowanego przełącznika do pracy z oferowanym modelem przełącznika, co oznacza, że dostarczony model wkładki musi znajdować się w ofercie sprzedaży producenta przełącznika lub na oficjalnej opublikowanej przez producenta przełącznika liście kompatybilności.
c) Niedopuszczalne jest dostarczenie zamiennych wkładek niecertyfikowanych, których montaż mógłby spowodować utratę gwarancji producenta przełącznika lub jakiekolwiek problemy konfiguracyjne

4. Możliwość konfiguracji portów typu: D_Port, E_Port,F_Port, M_Port; Przełącznik musi mieć obsługę trybu NPIV na portach
5. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
6. Przełącznik Fibre Channel musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC
7. Przełącznik Fibre Channel musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
   a) mechanizm tzw. Switch Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa urządzeń FC do podłączenia do przełącznika fabric
   b) mechanizm tzw. Port Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa hostów i urządzeń storage FC do podłączenia do portu przełącznika
   c) uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów FCAP
   d) uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
   e) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
   f) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
   g) definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+
   h) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
   i) obsługa SNMP v1 oraz v3
   j) wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
   k) wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
8. Przełącznik Fibre Channel musi umożliwiać rozbudowę o agregację połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.
9. Przełącznik Fibre Channel musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
10. Przełącznik Fibre Channel musi umożliwiać rozbudowę instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s.
11. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika
12. Przełącznik Fibre Channel musi mieć możliwość konfiguracji przez:
    a) HTTP/HTTPS, poprzez SSH, obsługa SNMP v1/v3,
    b) możliwość wysyłania logów na zewnętrzny serwer syslog,
    c) Osobny interfejs sieciowy 10/100/1000 Mbps Ethernet RJ-45 pozwalający na zarządzanie przełącznikiem
    d) Port szeregowy (RJ-45) pozwalający na bezpośrednie podłączenie się do przełącznika
13. Możliwość rozbudowy w przyszłości o poniższe licencje (dla każdego przełącznika)
    a) Fabric Vision
    b) ISL Trunking
    c) Extended Fabric
14. Możliwość diagnozowania z poziomu przełącznika połączeń światłowodowych, Możliwość pomiaru połączenia (prędkość, opóźnienia, dystans), wbudowany generator przepływu danych, możliwość wykonywania poleceń FC ping, Pathinfo (FCtraceroute), możliwość podglądu ramek, monitorowanie stanu łącz, monitorowanie stanu urządzenia
15. Preferowany sposób montażu i kierunek przepływu chłodnego powietrza
    a) Montaż w tylnej części szafy rack

b) Przepływ powietrza chłodzącego przez przełącznik od tyłu urządzenia w kierunku interfejsów.
c) Wraz z przełącznikiem wymagane jest dostarczenie wszelkich elementów i akcesoriów niezbędnych do prawidłowego zamontowania przełącznika w szafie RACK oraz prawidłowej cyrkulacji powietrza (np. szyny montażowe, śruby itp.)

16. Urządzenie musi współpracować z krajową siecią energetyczną o parametrach znamionowych: 230 V, 50 Hz.
17. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 77W.
18. Chłodzenie aktywne, zapewnione działanie urządzenia przy 2 uszkodzonych wentylatorach.
19. Oferowane produkty (urządzenia, sprzęt) muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE
20. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
21. Wraz z każdym przełącznikiem należy dostarczyć 10 szt. okablowania OM4 o długości minimum 2 metrów

VII. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE KLASTRA WIRTUALIZACJI

Klaster wirtualizacji będzie przeznaczony na uruchomienie systemów SIEM oraz SOAR będących częścią tego zamówienia.

Dostarczony klaster (4 sztuki) przełączników SAN musi spełniać następujące wymagania:

1. Klaster wirtualizacji musi składać się z minimum 4 serwerów fizycznych.
2. Każdy z serwerów musi być wyposażony w 2 procesory x86 wyposażony w 32 rdzenie fizyczne i z bazowym taktowaniem minimum 2.4 Ghz i osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 540 punktów, dla testu oferowanego modelu serwera z 2 procesorami.
3. Każdy z serwerów musi być wyposażony w Min. 640 GB RDIMM DDR5 5600 MT/s w modułach pamięci o pojemności min. 32GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
4. Min. 3 aktywne gniazda PCI-Express generacji 5, x16 (szybkość slotu – bus width) w tym dwa nieobsadzone.
5. Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji.
6. Serwer bezklatkowy z możliwością rozbudowy/rekonfiguracji w przyszłości serwera do 10 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy.
7. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatok dyskowych SFF gotowe do instalacji dysków SAS/SATA/SSD/NVMe 2,5” typu Hot Swap.
8. Zainstalowane min. 2 szt. dysków SSD NVMe 480GB niezajmujących wnęk na dyski twarde, pracujące w konfiguracji ze sprzętowym RAID 1.
9. Serwer wyposażony w kontroler software dla dysków SATA, obsługujący poziomy: RAID 0, 1, 5, 10.
10. Możliwość zastosowania/wymiany kontrolera na kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe.
11. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
12. Dwie dwuportowe karty 10/25GbE nie zajmujące gniazd opisanych w sekcji „sloty rozszerzeń”.
13. Jedna karta dwuportowa 32Gb FC z wkładkami SR.
14. Jedna karta dwuportowa 1GbE z interfejsem RJ45
15. Zintegrowana karta graficzna
16. 5 x USB, z czego min. 4szt. w wersji USB 3.2 oraz jeden port USB 2.0,
17. 1x VGA
18. 2 szt., typu Hot-plug, redundantny, każdy o mocy minimum 900W.
19. Zestaw wentylatorów redundantnych typu hot-plug
20. Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
21. Serwer wyposażony w moduł TPM 2.0.
22. Niezależna od systemu operacyjnego karta, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:
    a) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe

b) praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
c) dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port karty sieciowej serwera
d) dostęp do karty możliwy z poziomu przeglądarki webowej (GUI), z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP), z poziomu skryptu (XML/Perl), poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
e) wbudowane narzędzia diagnostyczne
f) zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
g) obsługa mechanizmu remote support- automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
h) wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
i) przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
j) uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu
k) obsługa zdalnego serwera logowania (remote syslog)
l) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów
m) mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
n) funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
o) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
p) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
q) zdalna aktualizacja oprogramowania (firmware)
r) zarządzanie grupami serwerów, w tym:
    a. tworzenie i konfiguracja grup serwerów
    b. sterowanie zasilaniem (wł/wył)
    c. ograniczenie poboru mocy dla grupy (power capping)
    d. aktualizacja oprogramowania (firmware)
    e. wspólne wirtualne media dla grupy
s) możliwość równoczesnej obsługi przez 6 administratorów
t) autentykacja dwuskładnikowa (Kerberos)
u) wsparcie dla Microsoft Active Directory
v) obsługa SSL i SSH
w) enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli
x) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API
y) wsparcie dla Integrated Remote Console for Windows clients
z) możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)

23. Wsparcie certyfikowane przez producenta dla systemów operacyjnych i systemów wirtualizacyjnych
    a) Microsoft Windows Server 2019, 2022,
    b) Ubuntu 20.04 LTS, 22.04 LTS,
    c) Red Hat Enterprise Linux (RHEL) 8.6, 9.0,
    d) VMware ESXi 7.0 U3, 8.0, 8.0 U1/U2.
24. . Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające że sprzęt produkowany jest zgodnie z normami ISO 9001 oraz ISO 14001.
25. Deklaracja zgodności CE.

VIII. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE OPROGRAMOWANIA WIRTUALIZACJI

Oprogramowanie wirtualizacji będzie przeznaczone na uruchomienie i utrzymanie systemów SIEM i SOAR będących częścią przedmiotu zamówienia.

1. Wszystkie licencje zaoferowanego oprogramowania do wirtualizacji muszą być licencjami subskrypcyjnymi, tj. licencja na określony czas, wskazany w formularzu technicznym wraz ze wsparciem technicznym do tych licencji świadczonym przez producenta zaoferowanego oprogramowania. Liczba licencji musi uwzględniać parametry serwerów do wirtualizacji (4 serwerów dwuprocesorowych z procesorami trzydziestu dwu rdzeniowymi).
2. Wszystkie wymagane poniżej komponenty/moduły muszą pochodzić od jednego producenta oprogramowania.

3. Licencje zaoferowanego oprogramowania muszą być zaoferowane w formie „per core” fizyczny procesora fizycznego.
4. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
5. Zaoferowane oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
6. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 700MB pamięci operacyjnej RAM serwera fizycznego.
7. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera.
8. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych
9. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM.
10. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
11. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
12. Zaoferowane oprogramowanie musi wspierać minimum następujące systemy operacyjne: Windows Server 2012/2016/2019/2022, Windows 8/10/11, RHEL 6/7/8/9, SLES 12/15, Debian 10/11, CentOS 7/8, Ubuntu 16/18/20/22, Photon OS 2/3/4, Oracle Linux 6/7/8/9, FreeBSD 12/13.
13. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione.
14. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
15. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość).
16. Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”
17. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
18. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
19. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
20. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
21. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji aż do 4096 portów
22. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
23. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
24. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE poprzez agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
25. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek

26. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
27. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
28. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
29. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
30. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. High Availability)
31. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
32. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
33. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
34. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
35. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
36. Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software Defined Network).
37. Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader
38. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
39. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10, Microsoft Windows Server 2016 oraz Microsoft Windows Server 2019
40. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
41. Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
42. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
43. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola

zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku

44. Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
45. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
46. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
47. Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
48. Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.
49. Zaoferowane oprogramowanie musi mieć możliwość utworzenia, poprzez API, maszyny wirtualnej jako tzw. Instant Clone poprzez klonowanie działającej maszyny wirtualnej w wyniku którego powstanie nowa działająca maszyna wirtualna identyczna z klonowaną. Nowa maszyna wirtualna musi powstawać w pamięci operacyjnej wirtualizatora
50. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra, musi mieć możliwość monitorowania i wyświetlania za pomocą grafu w konsoli bieżącego poboru energii elektrycznej dla hosta wirtualizacyjnego oraz dla maszyn wirtualnych na nim posadowionych
51. Ilość instancji zaoferowanego oprogramowania do zarządzania klastrem wirtualizacyjnym musi być równa liczbie fizycznych core zaoferowanych w oprogramowaniu do wirtulizacji mocy obliczeniowej
52. Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się, aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja w/w virtaul appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.
53. Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
54. Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
55. Zaoferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek minimum Mozilla Firefox oraz Chrome) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5
56. Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami VMware vSphere.
57. Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz http.
58. Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage).
59. Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5
60. Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
61. Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
62. Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości do 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
63. Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. High Availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.

64. Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
65. Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory.
66. Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

IX.MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE DLA SYSTEMU SIEM

1. Rozwiązanie SIEM musi zapewniać skalowalną architekturę spełniającą następujące wymagania:
   a) wszystkie elementy odpowiedzialne za zbieranie informacji, od tego miejsca określane jako Kolektory, mogą być dostarczone tylko w postaci rozwiązań wirtualnych z możliwością migracji/instalacji na platformach sprzętowych również pochodzących od tego samego producenta
   b) zadaniem kolektorów jest przesyłanie monitorowanych danych (np. zdarzeń) do warstwy je przechowującej i korelującej
   c) w wypadku awarii komunikacji pomiędzy warstwą przechowującą i korelującą a kolektorami muszą one mieć możliwość buforowania otrzymanych informacji:
      a. w wypadku awarii komunikacji pomiędzy warstwą przechowującą i korelującą a kolektorami muszą one mieć możliwość buforowania otrzymanych informacji
      b. system SIEM powinien mieć możliwość definiowania rozmiaru bufora dla zdarzeń otrzymywanych przez kolektor oraz monitorowania jego zajętości
   d) kolektory muszą mieć możliwość ograniczenia ilości zdarzeń przesyłanych do klastra SIEM
   e) kolektory muszą mieć możliwość kompresowania danych przesyłanych do warstwy przechowującej i korelującej
   f) kolektory muszą mieć możliwość ograniczania przepustowości, z którą zdarzenia są przesyłane do warstwy przechowującej i korelującej
   g) kolektory muszą mieć możliwość działania również w trybie niewymagającym bezpośredniej komunikacji z warstwą zarządzającą, bez połączenia z Internetem, komunikując się z innymi kolektorami lub warstwą korelującą z wykorzystaniem portu 514 UDP. Połączenie to musi być jednokierunkowe.
   h) komunikacja pomiędzy warstwą przechowującą i korelującą musi odbywać się z wykorzystaniem szyfrowanego protokołu HTTPS. Musi odbywać się ona w kierunku od kolektorów do warstwy przechowującej i korelującej dla przesyłanych zdarzeń
   i) w wypadku awarii kolektora, kolektor zastępczy może być uruchomiony poprzez jego zarejestrowanie w warstwie przechowującej i korelującej. Konfiguracja (zarządzanie) kolektorów nie odbywa się indywidualnie, lecz są one centralnie zarządzane. Nie mogą one posiadać żadnych parametrów konfiguracyjnych poza adresami IP, nazwą kolektora oraz wymaganymi poświadczeniami, które byłyby wymagane w celu uruchomienia kolektora zastępczego
   j) kolektory muszą mieć możliwość pracy w trybie wysokiej dostępności. W tym trybie urządzenia pracować muszą w trybie równoważenia obciążenia dla odpytywanych systemów źródłowych (tryb aktywnego odpytywania) a dla otrzymywanych logów np. poprzez protokół syslog, musi istnieć redundancja w trybie aktywny-pasywny.
   k) wydajność kolektora nie może być mniejsza niż 5 000 EPS (zdarzeń na sekundę odbieranych w trybie ciągłym)
   l) kolektory muszą być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu NetFlow
   m) poszczególne kolektory muszą być wstanie automatycznie aktualizować nowe parsery wtedy, gdy zostaną one zaktualizowane w centralnym systemie zarządzającym rozwiązaniem SIEM
   n) kolektory mają mieć możliwość aktualizacji wersji swojego oprogramowania z poziomu warstwy zarządzającej
   o) rozwiązanie SIEM ma posiadać możliwość aktualizacji online dla parserów, reguł, raportów oraz typów wspieranych urządzeń. Aktualizacja ta musi być niezależna od oprogramowania systemowego (OS, funkcje wykonawcze, etc.) które ma posiadać swoje wersjonowanie. Zmiany dokonane w kolejnych wersjach powinny być ewidencjonowane w oficjalnej dokumentacji
   p) rozwiązanie ma posiadać możliwość zarządzania wieloma instancjami SIEM przy pomocy dedykowanej konsoli zarządzającej pochodzącej od tego samego producenta. Funkcjonalność ta może wymagać dodatkowej licencji.
2. Warstwa przechowywania i korelacji danych, określana jako Klaster SIEM, ma spełniać następujące wymagania:
   a) implementacja ma być zrealizowana w oparciu o maszyny wirtualne (VA - Virtual Appliance) z możliwością migracji/instalacji na platformach sprzętowych również pochodzących od tego samego producenta

b) w przypadku przechowywania danych na dysku lokalnym lub udziale NFS ma być możliwe stworzenie architektury redundantnej w której podstawowa instalacja rozwiązania SIEM podczas regularnej pracy wykonuje wszystkie operacje produkcyjne, zaś instalacja backupowa synchronizuje wszystkie dane i w razie awarii jest w stanie przejąć funkcjonowanie środowiska SIEM, możliwe ma być również stworzenie architektury active-active dla warstwy zarządzającej
c) rozwiązanie ma wspierać nie mniej niż poniżej wymienione środowiska wirtualizacyjne:
   a. VMware
   b. Hyper-V
   c. KVM
   d. AWS
   e. Azure
d) klaster SIEM musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych (Virtual Appliance - VA). Wspomniana skalowalność ma być realizowana również poprzez:
   a. przeprowadzaną w czasie rzeczywistym, w pamięci rozwiązania, dystrybuowaną pomiędzy elementy klastra korelację reguł
   b. dystrybuowanie pomiędzy elementami klastra SIEM raportowania oraz analizy danych. Sam mechanizm dystrybucji musi być całkowicie przeźroczysty z perspektywy użytkownika, tak aby nie musiał on decydować który z elementów ma być odpowiedzialny za wykonanie poszczególnych zadań
e) klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej
f) klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)
g) dane zbieranych zdarzeń (events) mogą być gromadzone na dyskach maszyn wirtualnych lub udziale NFS podczas działania w oparciu o pojedynczą maszynę wirtualną lub też z możliwością wykorzystania NFS w sytuacji pracy w trybie klastra SIEM (wiele maszyn wirtualnych – VA).
h) klaster SIEM musi mieć możliwość obsłużenia (potencjalną możliwość docelowego wyskalowania do) nie mniej niż 500 tysięcy EPS. Konfiguracja taka musi być przedstawiona w oficjalnej dokumentacji producenta rozwiązania.
i) klaster SIEM musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych
j) rozwiązanie SIEM nie może wymagać zastosowania dodatkowej przestrzeni dyskowej i/lub warstwy służącej do filtrowania lub wysyłania podzbiorów danych przesyłanych od kolektorów do warstwy korelującej w przypadku korzystania z dysków lokalnych lub udziału NFS
k) zebrane dane muszą być przechowywane w sposób skompresowany
l) system musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji
m) klaster SIEM nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP. Musi być możliwy wybór zastosowanej bazy danych do przechowywania zbieranych zdarzeń spośród przynajmniej trzech różnych technologii z czego co najmniej jedna pochodzi od tego samego producenta
n) w przypadku stosowania struktury OLAP możliwe powinno być obsłużenie warstwy zarządzania zapisem danych oraz ich przechowywania i wyszukiwania na jednej, dwóch lub trzech dedykowanych warstwach maszyn fizycznych bądź wirtualnych klastra SIEM. Dopuszczalne są następujące scenariusze:
   c. wszystkie warstwy działają w ramach jednej maszyny
   d. dedykowane maszyny do pracy jako warstwa zarządzania zapisem danych oraz dedykowane maszyny do zapisu i wyszukiwania danych
   e. dedykowane maszyny do pracy jako warstwa zarządzania zapisem danych, dedykowane maszyny do pracy jako warstwa zapisu danych oraz dedykowane maszyny do wyszukiwania danych
   f. Musi istnieć możliwość konfiguracji warstwy zarządzania jako klastra złożonego z większej liczby instancji, nie mniejszej niż 3, zabezpieczającego przed awarią tej funkcji.
   g. Musi istnieć możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania.

h. Musi istnieć możliwość zbudowania struktury rozproszonej, aby zapewnić większą wydajność zapisu i wyszukiwania.

o) Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, zdarzeń i innych ustrukturyzowanych informacji

p) Maszyny wirtualne systemu SIEM mają działać w oparciu o system Linux który ma mieć możliwość aktualizacji. Aktualizacje zarówno rozwiązania SIEM jak i bazowego systemu operacyjnego muszą być dostarczane przez producenta rozwiązania w wygodnej formie pliku aktualizacyjnego

3. Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż:

a) aktywne wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich metod pobierania zdarzeń jak:
   a. SNMP
   b. Syslog
   c. Windows Management Instrumentation (WMI) i Open Management Infrastructure (OMI)
   d. Microsoft RPC
   e. Cisco SDEE
   f. Checkpoint LEA
   g. JDBC
   h. VM SDK
   i. JMX
   j. Telnet
   k. SSH
   l. NetFlow
   m. HTTPS
   n. IMAP
   o. IMAP over SSL
   p. POP3
   q. Kafka API
   r. import z pliku CSV
   s. import z pliku PCAP
   t. REST API

b) zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP, TCP, UDP, ICMP, JDBC, LDAP, SMTP, IMAP, POP3, POP3S, SSH, HTTP, HTTPS. Wyniki powyższego monitoringu mają dawać możliwość obliczenia poziomu dostępności danej usługi (np. procentowego).

c) wykryte urządzenie ma posiadać swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB) w ramach dostarczonego rozwiązania SIEM co jednocześnie ma umożliwiać prezentację następujących informacji (nie mniej niż):
   a. wersja oprogramowania/firmware/systemu operacyjnego
   b. numer seryjny urządzenia
   c. skonfigurowane interfejsy wraz z:
      i. nazwą interfejsu
      ii. adresem IP oraz podsiecią
      iii. statusem interfejsu (włączony, wyłączony)
      iv. informacją o skonfigurowanym poziomie bezpieczeństwa
      v. prędkością interfejsu
      vi. możliwością edycji nazwy oraz prędkości interfejsu
   d. procesach działających na urządzeniu lub systemie operacyjnym
   e. alarmach w przypadku zmiany statusu procesu np. jego uruchomienia lub zatrzymania

d) możliwość automatycznego przypisania do grupy poszczególnych typów urządzeń znajdujących się w CMDB, np. grupa serwerów Windows, grupa rozwiązań firewall, etc.

e) automatyczne wykrywanie aplikacji działających na poszczególnych urządzeniach. Wymagane jest aby baza urządzeń (CMDB) miała możliwość konfiguracji grup aplikacji celem automatycznego umieszczania w nich poszczególnych urządzeń, np. grupa aplikacyjna "IIS Servers" wyświetla wszystkie urządzenia z uruchomionymi usługami Microsoft IIS. Grupy typów urządzeń jak i grupy aplikacyjne muszą być dostępne do raportowania, analityki korelacyjnej oraz wyszukiwania informacji (zdarzeń, przepływów, wydajności, itp.)

f) wymagane jest, aby rozwiązanie SIEM posiadało wbudowany szablon (template), który po przeprowadzeniu aktywnego wykrywania urządzeń będzie pozwalał na automatyczne określenie jakiego rodzaju dane będą z nich zbierane oraz jaki będzie interwał ich pobierania

g) Monitorowanie metryk wydajnościowych ma dotyczyć nie mniej niż:
   a. utylizacji interfejsów sieciowych, występujących tam błędów, ilości wysłanych i odebranych danych (np. bajtów)
   b. obciążenia CPU
   c. wykorzystania pamięci
   d. wykorzystania przestrzeni dyskowej

e. utylizacji poszczególnych procesów
h) pobieranie informacji o zdarzeniach w oparciu udostępniany przez monitorowane systemy mechanizm API
4. Rozwiązanie SIEM musi dostarczać zunifikowane narzędzia analityczne dzięki którym możliwe jest wykonywanie zapytań w oparciu o ten sam język zarówno dla logów/zdarzeń zbieranych z urządzeń jak i dla danych wydajnościowych
5. Wymagane jest, aby kolektory systemu SIEM pozwalały na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania
6. Zarówno dane w stanie surowym jak i te sparsowane lub wzbogacone muszą być możliwe do przesłania do rozwiązania SIEM z kolektorów
7. Przetwarzanie danych związanych z poszczególnymi zdarzeniami (events) wykonywane jest poprzez parsery systemowe
8. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów
9. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)
10. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)
11. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:
    a) zdolność do definiowania wzorców które powtarzają się jako zmienne
    b) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych
    c) zdolność do testowania poszczególnych funkcji
    d) zdolność do przekształcania danych w trakcie ich parsowania
12. Funkcjonalność parsowania w SIEM musi mieć możliwość uzupełniania informacji w kolejnych zdarzeniach na podstawie wcześniejszego logu. Przykład zastosowania: w pierwszym zdarzeniu logowania występuje informacja o adresie źródłowym oraz identyfikator sesji użytkownika. W kolejnym zdarzeniu innego typu brak jest informacji o adresie IP. Parser musi mieć możliwość uzupełnienia tego pola w oparciu o wspólną wartość sesji oraz adres przekazany w pierwszym zdarzeniu.
13. Musi istnieć możliwość monitorowania urządzeń bez wykorzystania aplikacji typu agent oraz poprzez SSH, telnet, WMI, OMI, JMX oraz PowerShell
14. Rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu aplikacje typu agent
15. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:
    a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli systemu SIEM
    b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows
    c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application
    d) zdolność do monitorowania integralności plików
    e) zdolność do monitorowania rejestru systemowego
    f) zdolność do monitorowania urządzeń zewnętrznych (removable devices)
    g) zdolność do wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów
    h) zdolność do wykonywania poleceń WMI wraz z odsyłaniem wyniku ich działania w postaci logów
    i) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS
    j) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu
    k) zdolność do monitorowania takich parametrów jak obciążenie CPU, zajętość RAM, zajętość dysku, obciążenia sieci, działających aplikacji
    l) agent Windows musi mieć możliwość buforowania zbieranych zdarzeń w wypadku utraty komunikacji z pozostałymi elementami klastra SIEM
    m) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS
    n) Monitorowanie zainstalowanych w systemie certyfikatów SSL co najmniej w zakresie:
        a. Dodanie lub skasowanie certyfikatu
        b. Ostrzeżenie przed wygaśnięciem certyfikatu na co najmniej 30 dni przed datą ważności
        c. Wykrywanie certyfikatów typu „self-signed”
        d. Raportowanie o wygaśniętych certyfiatach
    o) Wsparcie dla technologii osquery (link: https://osquery.readthedocs.io/en/latest). SIEM musi posiadać predefiniowane zapytania osquery oraz umożliwiać budowanie własnych zapytań.

Wyniki zapytań muszą umożliwiać wykonanie korelacji, monitorowania oraz raportowania. Do wykorzystania tej technologii musi wystarczyć instalacja samego agenta, bez dodatkowych zabiegów administracyjnych na monitorowanej maszynie.

16. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości:
    a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli systemu SIEM
    b) możliwość zbierania logów z wykorzystaniem protokołu syslog
    c) możliwość zbierania logów z plików tekstowych
    d) zdolność do monitorowania integralności plików
    e) zdolność do monitorowania pliku w oparciu o jego sumę kontrolną
    f) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu
    g) zdolność do monitorowania takich parametrów jak obciążenie CPU, zajętość RAM, zajętość dysku, obciążenia sieci, działających aplikacji
17. System SIEM musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar
18. System musi posiadać co najmniej 2400 gotowych reguł korelacyjnych wprowadzonych przez producenta.
19. Aktualizacja reguł korelacyjnych przygotowywanych przez producenta musi być wykonywana gotowym i wygodnym mechanizmem w interfejsie graficznym. Obowiązkowe jest oddzielenie tego typu aktualizacji od aktualizacji systemu
20. System SIEM musi umożliwiać uruchomienie reguł korelacyjnych na danych historycznych w trybie wsadowym.
21. System SIEM musi umożliwiać import reguł korelacyjnych w formacie SIGMA co najmniej za pomocą: linku URL gdzie znajduje się źródłowa reguła, wgrania pliku zawierającego definicję reguły, wprost wpisanie treści w składni SIGMA YAML.
22. System SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI
23. System SIEM musi być w stanie wykryć usługi Active Directory oraz LDAP oraz wyświetlać informacje o strukturze katalogowej drzewa w GUI
24. Musi istnieć możliwość wykorzystania struktury katalogowej drzewa LDAP jako warunku podczas tworzenia raportów i w ramach pozostałych mechanizmów analitycznych
25. Muszą być wspierane zewnętrzne metody uwierzytelniania użytkowników SIEM, nie mniej niż:
    a) Active Directory lub LDAP
    b) RADIUS
    c) SAML
26. Musi istnieć integracja z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds – TI):
    a) wsparcie dla plików CSV musi być wykonywalne z wykorzystaniem interfejsu graficznego GUI
    b) definicje w ramach integracji muszą zawierać nie mniej niż:
        a. adresy IP
        b. domeny
        c. sumy kontrolne (hash)
        d. adresy URL
    c) wymagane jest, aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 200 tysięcy wpisów
    d) wraz z systemem SIEM musi być dostarczony, już zintegrowany, zestaw komercyjnych baz zagrożeń pochodzących od tego samego producenta. Producent musi mieć własny zespół analityczny, tworzący wspomniane bazy
    e) wraz z systemem SIEM musi być wspierany, już zintegrowany, zestaw baz zagrożeń niekomercyjnych (open source)
    f) system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data)
    g) system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi
    h) system musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal, w tym również pochodzących od producenta samego systemu SIEM
    i) system musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla wbudowanych reguł. Reguły dostarczone przez producenta muszą być skatalogowane według wspomnianej nomenklatury jak również skatalogowane muszą być generowane przez nie alarmy. Ilość reguł wskazujących na taktyki MITRE ma wynosić nie mniej niż 1000. Należy rozdzielić podział na matrycę MITRE ATT&CK dla systemów IT oraz ICT.
27. System SIEM musi mieć możliwość analizowania i odpytywania o zdarzenia w widoku analitycznym w trybie strumieniowym (streaming mode), w taki sposób, że raport docelowy dotyczący analizowanych zdarzeń wykonywany jest przed ich zapisaniem na dysk twardy
28. Rozwiązanie SIEM musi dostarczać bez dodatkowych opłat następujące rodzaje raportów:

a) PCI-DSS
b) HIPAA
c) SOX
d) NERC
e) FISMA
f) ISO
g) GLBA
a. GPG13
b. SANS Critical Controls

29. System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML
30. System SIEM musi pozwalać na zbieranie konfiguracji urządzeń, identyfikowanie zmian w nich następujących wraz z możliwością porównywania poszczególnych wersji obok siebie w interfejsie GUI. zmian konfiguracji na NGFW przez operatora SIEM poprzez wyświetlenie konfiguracji tekstowej nowej i wybranej wcześniejszej wersji jednocześnie. Zmiany muszą być zaznaczone wyraźnie np. kolorem (dodano, usunięto, zmieniono).
31. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji
32. Dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji:
    a) Bar
    b) Pie
    c) Line
    d) Table
    e) Combination (line and table view)
    f) Treemap
    g) Scatter graph
    h) Single values
    i) Gauges
    j) Geographical Map
    k) wartości graniczne (thresholds) w kolorach czerwonym, bursztynowym oraz zielonym mogą być definiowane w razie potrzeby na poszczególnych wykresach
33. Notyfikacje oraz zarządzanie incydentami. System SIEM musi:
    a) posiadać narzędzia pozwalające na samodzielne tworzenie polityk informujących o incydentach
    b) pozwalać na nadawanie etykiet (tagów) poszczególnym incydentom oraz powinno pozwalać na wyszukiwanie w oparciu o nie
    c) posiadać możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty musi być możliwa w oparciu o role z podziałem na użytkowników mających pełne prawa do uruchamiania skryptów i na użytkowników zgłaszających żądanie uruchomienia skryptu, które to żądanie musi być zatwierdzone przez użytkownika nadrzędnego
    d) posiadać możliwość integracji w oparciu o API z zewnętrznymi systemami do obsługi zgłoszeń (ticketingsystems) takimi jak Jira, ManageEngine, ServiceNow, ConnectWise oraz Remedy
    e) mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system)
    f) mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów
34. Analityka. System SIEM musi mieć możliwość:
    a) wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłowów
    b) zagnieżdżania wyników wyszukiwań w oparciu o operatory IN oraz NOT IN
    c) wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych
    d) wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne.
    e) wyszukiwania w oparciu o zapytania wstępne uruchamiane zgodnie harmonogramem
    f) wyszukiwania w oparciu o niemniej niż następujące operatory: include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex
    g) podejmowania w czasie rzeczywistym działań w oparciu o złożone wzorce zdarzeń
        a. w przypadku prostych zapytań musi na przykład być możliwe określenie wartości progowej (threshold) ilości zdarzeń X w określonym przedziale czasowym Y z Z wybranych wartości
        b. w przypadku zapytań przekrojowych wspierających filtry typu Boolean musi być możliwe:

- stworzenie wzorców zapytań za określony przedział czasu z wykorzystaniem operatorów takich jak: AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED_BY
- każdy z wzorców może być filtrowany i agregowany z wykorzystaniem operatorów takich jak: AVG, MAX, MIN, COUNT and COUNT DISTINCT
- ustalane wartości graniczne (thresholds) mogą być statyczne lub też mogą być otrzymywane jako rezultat analizy statystycznej

h) analiza statystyczna i alarmowanie w oparciu o zdarzenia musi mieć możliwość działania w oparciu o:
   - średnie kroczące (movingaverages)
   - odchylenia standardowe (standard deviations)
   - w wypadku przekroczenia statystycznej wartości granicznej (statistical threshold) musi zostać wygenerowany alert w czasie zbliżonym do rzeczywistego

i) wykorzystania mechanizmów Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym, gdzie system SIEM sam decyduje o wyborze optymalnego. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.

j) wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenia reguł

k) tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną

l) możliwości eksportowania raportów do formatów CSV, PDF i RTF

m) tworzenia raportów z wykorzystaniem graficznego edytora pozwalającego na podgląd pliku PDF przed jego wygenerowaniem

n) wyszukiwania zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego

o) wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej

p) skalowania możliwości analitycznych poprzez dodawanie do systemu SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego klastra SIEM

q) automatycznego korelowania użytkownika z jego lokalizacją i adresem IP:
   a. musi istnieć możliwość tworzenia raportów i wyszukiwania użytkownika w połączeniu z jego adresem IP oraz lokalizacją. Lokalizacja może oznaczać port na przełączniku sieciowym, adres MAC lub połączenie VPN
   b. musi istnieć możliwość wzbogacania zdarzeń (events) przy których dane użytkownika pozbawione są informacji o adresie IP
   c. wykorzystanie funkcjonalności lokalizacji adresu IP (Geo IP) w oparciu o bazę pochodzącą od tego samego producenta
   d. Musi istnieć możliwość łączenia różnych kont takich jak login w active directory, adres e-mail, nazwa konta w usługach chmurowych dla jednego użytkownika w ramach funkcji tzw aliasu.

r) możliwość wykrywania zdarzeń IPS falsepositive w oparciu o integrację z zewnętrznymi skanerami podatności

35. Zarządzanie incydentami: system SIEM musi posiadać wbudowane funkcjonalności zarządzania incydentami co najmniej w zakresie:
    a) Łączenia podobnych incydentów w jedno zgłoszenie
    b) Automatyczne przypisywanie nowych incydentów do operatorów
    c) Przypisywanie parametrów oczekiwanych czasów obsługi incydentu w zależności od jego wagi. Minimalne monitorowane parametry to czas przyjęcia i czas zamknięcia.
    d) Automatyczne eskalowanie opóźnionej obsługi incydentów
    e) Automatyczne zamykanie incydentów
36. Systemu SIEM musi mieć możliwość definicji zespołów obsługi incydentów. Każdy członek zespołu musi posiadać swój kalendarz pracy (dni pracy i dni niedostępności).
37. Musi istnieć możliwość wykorzystania zewnętrznych silników sztucznej inteligencji, np. OpenAI/ChatGPT-4 lub odpowiednika do prowadzenia dialogu operatora z systemem. Zakres otrzymywanych informacji nie może być mniejszy niż:
    a) Informacje o stanie operacyjnym systemu SIEM
    b) Informacje o znalezionych podatnościach
    c) Odpowiedzi dotyczące dokumentacji producenta oraz bazy wiedzy
    d) Analiza i rekomendacje dla logów i incydentów
    e) Pomoc w przygotowaniu raportów

38. System SIEM musi pozwalać na przesłanie dowolnych zebranych zdarzeń z wykorzystaniem protokołu KAFKA
39. Dla danych przechowywanych na dysku lokalnym lub udziale NFS system SIEM musi pozwalać na realizowane w oparciu o polityki archiwizowanie danych do innego udziału, takiego jak np. NFS
40. Integralność danych zapisywanych na dysku lokalnym lub udziale NFS związanych ze zdarzeniami musi być weryfikowalna z wykorzystaniem GUI w oparciu o przeliczenie sum kontrolnych, które obliczane były w momencie zapisywania danych o zdarzeniach na dysk systemu SIEM
41. System musi mieć możliwość uruchomienia w trybie zgodności z FIPS
42. Producent oferowanego systemu musi utrzymywać publicznie dostępną dokumentację.
43. Producent oferowanego systemu musi wspierać integrację z przynajmniej jednym rozwiązaniem typu SOAR, gdzie możliwe musi być co najmniej:
    a) uruchamianie procedur wykonawczych SOAR (tzw. Playbook) z poziomu SIEM
    b) wykonywanie operacji na systemach zintegrowanych z SOAR, np. pobranie listy zablokowanych adresów IP na firewall, dodanie do blokady adresu URL, zweryfikowanie reputacji IOC w serwisie internetowym.
44. Oferowany system musi znajdować się w raportach Gartnera co najmniej od 2018 roku
45. Dla systemu SIEM muszą być dostępne certyfikowane szkolenia w tym poprzez portal producenta
46. Dostarczony system musi obsługiwać poniższe źródła logów opisane w Załączniku do wymiarowania systemu SIEM.
47. Jeśli producent oferowanego systemu nie zapewnia obsługi wszystkich podanych źródeł to obowiązkiem dostawcy będzie zapewnienie wsparcia dla brakujących typów systemów w ramach wdrożenia. Wsparcie musi być zrealizowane w minimalnym zakresie:
    a) Pełna normalizacja logów (parsowanie)
    b) Jeśli zasadne to automatyczne wykrywanie
    c) Dedykowany zestaw monitorowania systemu (parametry oraz wartości progowe)
    d) Tam, gdzie to zasadne dodanie lub modyfikacja reguł korelacji.
48. System musi posiadać licencję na obsługę co najmniej ilość zdarzeń na sekundę wskazaną w formularzu ofertowym. Chwilowe przekroczenie wartości licencji nie może powodować utraty danych raportowanych przez źródła.
49. System musi posiadać architekturę, która będzie odporna na awarię jednego serwera fizycznego, dowolnego nośnika danych (np. dyski), zapisywać dane w co najmniej dwóch rozdzielnych przestrzeniach dyskowych.
50. Oferowany SIEM musi być wyposażony w subskrypcje reputacji wskaźników (IOC – indicator of compromise) od tego samego producenta co najmniej w zakresie: adresy IP, domeny, adresy URL. Informacje o reputacji muszą pochodzić z komercyjnego źródła, najlepiej tego samego producenta.
51. Licencje na system SIEM muszą być dostarczone w formie wieczystego użytkowania (ang: perpetual)
52. Wszelkie subskrypcje, gwarancja producenta muszą być ważne na okres wskazany w formularzu ofertowym od daty odbioru.

X. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE DLA SYSTEMU SOAR

1. Udostępnienie jednego interfejsu i platformy pochodzących od tego samego producenta dla zarządzania, orkiestracji bezpieczeństwem informatycznym jak i automatyzacji działań i zadań
2. Zarządzanie incydentami bezpieczeństwa
3. Zautomatyzowanie powtarzalnych zadań w ramach zespołu SOC
4. Identyfikacja i rozróżnienie zagrożeń od fałszywych alarmów
5. Poprawa parametrów działania zespołu SOC
6. Ułatwienie zarządzania pracą zespołu SOC
7. Ustandaryzowanie procesów i procedur postępowania
8. Wprowadzenie parametrów oraz ich pomiaru, służących do raportowania wydajności i skuteczności obsługi zdarzeń bezpieczeństwa zarówno przez zespół jak i mechanizmy automatyzujące
9. Zdecydowaną redukcję powtarzalnych działań pracowników na rzecz automatycznych kroków i całych procesów
10. System MUSI mieć możliwość instalacji w infrastrukturze Zamawiającego bez żadnego elementu wykonawczego, analitycznego lub innego znajdującego się poza infrastrukturą Zamawiającego.
11. System MUSI mieć możliwość domyślnej instalacji w środowisku wirtualizacyjnym i MUSI wspierać co najmniej środowiska producentów VMWare oraz Red Hat KVM.
12. System POWINIEN być dostarczony jako kompletny obraz do instalacji, zarówno systemu operacyjnego jak i oprogramowania. MUSI być dostępna opcja instalacji SOAR na własnym systemie operacyjnym Zamawiającego, co najmniej Red Hat.

13. Zamawiający wymaga aby licencje na dostarczany System SOAR były dostarczone w modelu licencji nieograniczonej czasowo wraz ze wsparciem technicznym producenta . Wsparcie producenta będzie wykupione przez Wykonawcę na okres wskazany w Formularzu ofertowym.
14. System MUSI posiadać licencjonowanie oparte o liczbę użytkowników jednocześnie korzystających z systemu – sprawdzanie powinno być realizowane w oparciu o jednoczesne aktywne sesje zalogowanych użytkowników.
15. System POWINIEN umożliwiać przypisywanie licencji na sesję dla kont imiennych, gdzie jedno konto zużywa jedną licencję oraz tworzenie kont wspólnych, które działają w ramach pozostałej puli dostępnych połączeń. Zmiana trybu licencji dla poszczególnych kont powinna być możliwa w dowolnym momencie.
16. System SOAR NIE MOŻE licencjonować lub ograniczać innych parametrów systemu, jak ilość wykonywanych akcji, liczba podłączonych konektorów, rozmiar dysku, itp.
17. System SOAR MUSI mieć możliwość szyfrowania danych zapisywanych na dysku lokalnym. Szyfrowanie takie musi być wspierane przez producenta oprogramowania, a sposób konfiguracji musi być opisany w publicznie dostępnej dokumentacji produktu.
18. SOAR MUSI mieć możliwość obsługi wielu organizacji w ramach jednej instalacji (multitenant). Informacje w ramach jednej organizacji MUSZĄ być odseparowane od pozostałych w ramach interfejsu i ról operatora.
19. System MUSI mieć możliwość wyboru wielu języków interfejsu graficznego GUI. Musi istnieć możliwość zaimplementowania języka polskiego.
20. System SOAR MUSI mieć możliwość pracy hybrydowej dla trybu obsługi wielu organizacji (multitenant), tzn. musi istnieć możliwość komunikacji z/do podległej organizacji zarówno bezpośrednio z centralnego systemu jak i lokalnie zainstalowanego systemu w obsługiwanej organizacji, który jest dedykowanym i wydzielonym elementem SOAR.
21. W ramach trybu obsługi wielu organizacji (multitenant) MUSI istnieć możliwość licencjonowania i tworzenia dedykowanych kont operatorów w ramach danej organizacji, którzy mają dostęp do danych tylko i wyłącznie w swoim zakresie.
22. System SOAR MUSI mieć możliwość instalacji oraz aktualizacji w trybie offline, tzn. bez dostępu systemu do Internetu. Wymaganie dotyczy również pracy z konektorami.
23. Producent systemu MUSI dostarczać aktualizacje obejmujące zarówno system operacyjny jak i oprogramowanie SOAR.
24. Aktualizacja konektorów NIE MOŻE powodować restartu systemu.
25. Aktualizacja istniejących w systemie konektorów i obsługiwanych przez producenta MUSI być realizowana z poziomu GUI systemu, bez konieczności uruchamiania innego interfejsu.
26. Aktualizacje MUSZĄ być widoczne w interfejsie systemu od momentu ich dostępności (dotyczy pracy w trybie online).
27. Rozwiązanie MUSI zawierać kreator wspomagający tworzenie niestandardowych integracji. Jednocześnie wszystkie istniejące integracje (konektory i ich akcje) muszą być edytowalne za pośrednictwem GUI, wraz z możliwością pracy nad kodem źródłowym, bez konieczności używania zewnętrznego IDE.
28. Konektory MUSZĄ posiadać funkcję automatycznej weryfikacji działania, tzn. muszą weryfikować poprawność ustawień i prawidłową współpracę z systemem integrowanym poprzez wykonywania aktywnych testów połączenia. Wynik weryfikacji MUSI być widoczny, a błędy muszą być logowane.
29. Wszystkie konektory MUSZĄ udostępniać swój kod dla administratora Zamawiającego z poziomu systemu. MUSI też być możliwa swobodna modyfikacja kodu oraz wersjonowanie konektora. MUSI być możliwość dodawania własnych akcji w ramach danego pakietu.
30. Tam gdzie to jest możliwe i zasadne konektory MUSZĄ wykorzystywać szyfrowane połączenia z systemem integrowanym, np. poprzez protokół SSL i weryfikację certyfikatu.
31. MUSI istnieć możliwość pisania własnych konektorów w języku python. Proces tworzenia nowego konektora MUSI być możliwy do realizacji w środowisku zewnętrznym jak i w ramach zainstalowanego systemu. SOAR MUSI posiadać możliwość importu konektorów z przygotowanego wcześniej archiwum.
32. Producent MUSI dostarczyć zestaw bibliotek SDK (j. ang: Software Development Kit) dla łatwego tworzenia własnych konektorów.
33. Oferowany system MUSI posiadać publicznie dostępne repozytorium dla integracji, konektorów, pakietów rozszerzeń np. GitHub. Repozytorium to MUSI być aktualizowane zarówno przez producenta jak i społeczność użytkowników.
34. Oferowany system MUSI posiadać publicznie dostępną dokumentację co najmniej w zakresie: instalacji i pierwszej konfiguracji, dokumentacji dla dostępnych w systemie konektorów, API, administracji systemem, ścieżki aktualizacji wersji, informacji o wydaniu (release notes), tworzenie konektorów oraz Playbook-ów.
35. Producent oferowanego systemu MUSI utrzymywać dedykowany (odrębny od wspomnianej dokumentacji) portal dla treści związanych z konfiguracją systemu obejmujący co najmniej: konektory, gotowe szablony konfiguracji, elementy interfejsu graficznego. Portal ten musi pozwalać na pobieranie wcześniej wymienionych, gotowych do importu modułów. Portal MUSI

być dostępny publicznie i NIE MOŻE wymagać jakichkolwiek opłat za korzystanie z zawartości.

36. Zamawiający wymaga, aby dla oferowanego systemu dostarczona była również wersja testowa. Wersja testowa POWINNA posiadać taką samą funkcjonalność i wersję jak produkcyjna. MUSI być możliwe uruchomienie więcej niż jednej instancji testowej.
37. System SOAR MUSI umożliwiać importowanie części konfiguracji lub interfejsu z innego systemu, np. testowego.
38. Interfejs graficzny MUSI udostępniać szatę kolorystyczną GUI co najmniej w jasnych barwach i ciemnych (darkmode).
39. System SOAR MUSI posiadać elastyczną możliwość integracji z zewnętrznymi systemami, najlepiej w formie konektorów, za pomocą dostępnych protokołów, nie mniej niż: API, SSH, Syslog, TAXII, SMTP, SOAP, IMAP, bazy danych, pliki w formatach XML, HTML i JSON, SMB, LDAP, SSL. Dla każdego integrowanego producenta MUSZĄ być dostępne akcje charakterystyczne dla danego rozwiązania. MUSI być możliwość instalacji tylko niezbędnych do działania konektorów.
40. SOAR MUSI posiadać graficzny interfejs budowania i symulacji Playbook-ów.
41. Edytor Playbook-ów MUSI udostępniać co najmniej następujące typy elementów wykonawczych. Wykonanie zadania przez użytkownika technicznego SOAR (personel SOC/CSIRT). Wykonanie zadania przez użytkownika biznesowego. Wykonanie automatycznego zadania w zintegrowanym z SOAR systemie bezpieczeństwa Zamawiającego. Wykonanie automatycznego zadania w elemencie infrastruktury teleinformatycznej Zamawiającego.
42. Projektowanie i wykonywanie Playbook-ów MUSI udostępniać możliwość złożonych ścieżek postępowania, w tym co najmniej: Ścieżek równoległych, Ścieżek alternatywnych, Ścieżek warunkowych
43. Playbook MUSI udostępniać możliwość budowania rozdzielnych ścieżek
44. postępowania na każdym jego etapie w zależności od parametrów wejściowych dodanego elementu.
45. Wykonywanie Playbook-ów MUSI udostępniać możliwość rozwidlania na wiele ścieżek i zbieżności wielu ścieżek w jednym elemencie.
46. SOAR MUSI udostępniać możliwość budowania nowych Playbook-ów na bazie już istniejących poprzez kopiowanie i edycję.
47. SOAR MUSI udostępniać możliwość wersjonowania Playbook-ów.
48. System SOAR MUSI posiadać możliwość importu do Playbook-ów workflow z narzędzia BPMN. MUSI być obsługiwany format pliku źródłowego XML i JSON.
49. SOAR MUSI udostępniać możliwość tworzenia Playbook-ów zagnieżdżonych tzn. korzystających z już istniejących, gdzie istniejący Playbook jest częścią utworzonego nowego playbook-a.
50. SOAR MUSI posiadać mechanizmy wyboru ścieżki/ścieżek w Playbook-ach na podstawie kontekstu danych/parametrów.
51. SOAR MUSI się integrować z zewnętrznymi systemami CTI (Cyber Threat Intelligence).
52. System MUSI posiadać warstwowy mechanizm przetwarzania obsługiwanych alarmów. Minimalny zakres to: stopień 1: przetwarzanie odebranych rekordów z zewnątrz zanim zostanie on zapisany w systemowych bazach danych (możliwe jest na przykład odrzucenie rekordu do dalszego przetwarzania); stopień 2: właściwe przetwarzanie procedur; stopień 3: działania po wykonaniu procedur (playbook), przez co możliwe jest na przykład zaawansowane łączenie podobnych rekordów z nowo utworzonym.
53. Producent SOAR MUSI dostarczać własną bazę CTI (Cyber Threat Intelligence) możliwą do uruchomienia w systememie.
54. System MUSI posiadać interfejsy pozwalające na integrację z rozwiązaniami CyberThreatIntelligence (STIX, TAXII).
55. Integracja z CTI MUSI umożliwiać pobieranie przez System SOAR informacji o aktualnych danych związanych z zagrożeniami występujących w cyberprzestrzeni (listy reputacyjne adresów IP, adresów DNS, skróty (sumy kontrolne) złośliwego oprogramowania oraz złośliwych plików, itp.).
56. System SOAR MUSI posiadać możliwość definiowania w sposób ustrukturyzowany danych o Incydencie w postaci artefaktów. Co najmniej MUSZĄ być wspierane domyślnie następujące rodzaje:
57. SOAR MUSI posiadać możliwość wprowadzania informacji o Incydentach różnymi interfejsami w tym co najmniej:
    a) Poprzez Operatora manualnie
    b) Poprzez integracje z systemem ServiceDesk (zdarzenie zakwalifikowane jako Incydent cyberbezpieczeństwa)
    c) Poprzez integracje z systemami bezpieczeństwa
    d) Przez SIEM
    e) Poprzez pocztę elektroniczną – dedykowane konto dla powiadomień

58. SOAR MUSI posiadać możliwość wprowadzania informacji o Incydentach różnymi interfejsami w tym co najmniej:
    a) pliki
    b) skróty danych w postaci SHA1, SHA256, MD5
    c) adresy IP
    d) adresy URL
    e) nazwy DNS
    f) Hostname
    g) Port
    h) Rejestr
    i) użytkownik
    j) proces
    k) adres email
59. System SOAR MUSI mieć możliwość dowolnego definiowania nowych typów artefaktów.
60. SOAR POWINIEN mieć możliwość tworzenia skryptów w co najmniej języku programowania PYTHON.
61. SOAR MUSI mieć domyślnie zdefiniowane co najmniej 5 stopni istotności Incydentów. Ilość stopni jak i ich nazwy POWINNY udostępniać możliwość definiowania.
62. SOAR MUSI mieć możliwość TAG-owania zdarzeń przekazywanych do SOAR, alertów, zadań i incydentów.
63. SOAR MUSI mieć możliwość definiowania SLA na poziomie alarmów i incydentów.
64. SOAR MUSI mieć możliwość definiowania ról w zakresie rozwiązywania, zarządzania i raportowania incydentów bezpieczeństwa.
65. SOAR MUSI mieć możliwość definiowania co najmniej pięciu rodzajów ról ze względu na uprawnienia
    a) Menadżer Incydentów
    b) Pracownik I linii SOC
    c) Pracownik II linii SOC
    d) Pracownik III linii SOC
    e) Użytkownik biznesowy
66. SOAR MUSI posiadać możliwość integracji z systemami SIEM w zakresie przekazywania informacji o Incydentach.
67. SOAR MUSI mieć możliwość załączania plików.
68. SOAR MUSI mieć możliwość zamieszczania komentarzy w zadaniach.
69. SOAR MUSI mieć możliwość cyklicznego uruchamiania Playbook-ów według ustalonego harmonogramu.
70. SOAR MUSI umożliwiać przechowywanie danych o Incydentach z pełną informacją o operacjach wykonanych w systemie w zadanym okresie czasu.
71. MUSI zawierać moduł zarządzania kryzysowego w postaci tzw. War Room, aby umożliwić współpracę między zespołami w wypadku wystąpienia krytycznych incydentów. War Room MUSI być tworzony ręcznie lub poprzez eskalację istniejącego incydentu.
72. SOAR Moduł War Room zapewniać interfejs agregujący całościową informację o rozwiązywanym incydencie szczególnej wagi w tym:
    a) Status incydentu
    b) Listę aktualnie wykonywanych zadań
    c) Wyniki wykonanych zadań
    d) Raport aktualnej sytuacji oraz plan kolejnych działań
73. SOAR MUSI mieć możliwość personalizowania widoków w interfejsach dla użytkowników.
74. SOAR MUSI posiadać mechanizmy integracji z systemami bezpieczeństwa oraz infrastrukturą teleinformatyczną w zakresie zdefiniowanym w Załączniku do wymiarowania systemu SIEM.
75. SOAR MUSI mieć możliwość definiowania cyklicznego generowania raportów.
76. SOAR MUSI posiadać mechanizmy logowania zdarzeń i operacji wykonywanych przez użytkownika.
77. SOAR MUSI posiadać mechanizmy uwierzytelniania w oparciu o Active Directory i protokół SAML.
78. Zarządzanie uprawnieniami MUSI być oparte o role.
79. SOAR MUSI posiadać mechanizmy uwierzytelnia wieloskładnikowego.
80. SOAR MUSI posiadać mechanizmy integracji z systemami PAM.
81. SOAR MUSI posiadać interfejs użytkownika udostępniany poprzez https.
82. SOAR MUSI mieć możliwość automatycznego powiązania i grupowania podobnych incydentów (np. ten sam docelowy adres IP, usługa itp.)
83. System SOAR MUSI posiadać wbudowaną funkcjonalność tworzenia i zarządzania zadaniami.
84. Wszystkie atrybuty widoku alarmów, takie jak nazwa, ważność, itp. MUSZĄ być konfigurowalne, aby użytkownicy mogli je dodawać lub usuwać z interfejsu. Ponadto MUSI istnieć możliwość tworzenia, modyfikowania i usuwania własnych niestandardowych atrybutów w dowolnym module systemu.

85. Rozwiązanie MUSI umożliwiać skorelowanie i powiązanie rekordu typu alert, incydent, IoC z innym rekordem w systemie, w tym z niestandardowymi typami rekordów, które użytkownicy sami definiują. Relacje MUSZĄ obejmować co najmniej modele „Wiele-do-wiele" i „Wiele-do-jednego"
86. Rozwiązanie MUSI mieć silnik przewidywania oparty na uczeniu maszynowym, który przewiduje wartości pól na podstawie danych historycznych. Zakres przewidywania uczenia maszynowego MUSI obejmować wszystkie moduły produktu: wbudowane (takie jak alerty, incydenty, wskaźniki, itd.) jak i niestandardowe.
87. Widok każdego modułu GUI MUSI być dowolnie konfigurowalny za pomocą szablonu widoku, który definiuje położenie każdego pola i widżetu.
88. System MUSI zapewniać funkcję globalnego wyszukiwania, która umożliwia analitykowi wyszukiwanie poprzez słowa kluczowe w całym systemie i we wszystkich modułach.
89. Interfejs użytkownika GUI MUSI oferować możliwość łączenia różnych rekordów razem (linkowanie). Rekordy mogą być między innymi: artefakty, zadania, War Room, użytkownicy, kampanie, assety, alarmy, załączniki, wiadomości e-mail, incydenty.
90. MUSI być możliwa eskalacja zgłoszenia ręcznie przez operatora lub automatycznie za pośrednictwem automatycznie uruchamianego Playbook-a, który może zastosować dowolną logikę jako warunek przed wykonaniem eskalacji zgłoszenia.
91. Incydenty, alarmy, artefakty, załączniki i moduły niestandardowe MUSZĄ udostępniać analitykom możliwość komunikowania się za pomocą komentarzy. Każda wiadomość wpisana przez analityka lub Playbook MUSI pozostać atrybutem rekordu, w którym został utworzony. Dodatkowo komentarze muszą umożliwiać:
    a) tworzenie ich prostym tekstem lub tekstem sformatowanym
    b) oznaczanie analityków w samym komentarzu, celem zwrócenia ich uwagi poprzez sposób typowy dla komunikatorów: @<nazwa konta>
    c) uruchamianie akcji
    d) obsługę tag-ów
    e) obsługę załączania plików
    f) zarządzanie dostępem do nich w oparciu o RBAC
92. System MUSI umożliwiać analitykowi analizę graficzną powiązań pomiędzy Incydentami i IOC. Graficzna korelacja MUSI być dostępna dla różnych typów rekordów np. assety, podatności, alarmy, incydenty.
93. Rozwiązanie MUSI być zintegrowane z MITRE ATTACK, przez którą to możliwe będzie wzbogacenie analizy incydentów o informacje takie jak: taktyki, analiza zagrożenia i sugestie dotyczące środków zaradczych.
94. System MUSI umożliwiać skonfigurowanie obowiązkowego uzupełnienia notatek przez operatora przed zamknięciem dochodzenia, dla incydentu obejmującego co najmniej sekcje:
    a) informacja podsumowująca
    b) następne kroki
    c) opis sposobu rozwiązania problemu
    d) Każde pole MUSI mieć możliwość wyboru konfiguracji: nieobowiązkowe, obowiązkowe, warunkowo obowiązkowe.
95. Obsługa incydentów MUSI wspierać oznaczanie fazy analizowanego ataku (kill chain phase). MUSI być możliwa zmiana definicji faz jak i ich ilości. Ustawiona faza w ramach incydentu POWINNA być reprezentowana graficznie.
96. Rozwiązanie MUSI mieć konfigurowalną funkcję zarządzania kolejkami obsługującą automatyczne przypisywanie alertów/incydentów/zadań do różnych grup obsługujących.
97. Rozwiązanie MUSI wyodrębnić artefakty (IP, URL, Domena, itp) z ponad 1500 typów plików takich jak MS Office, PDF, itd. Wyodrębnione artefakty muszą być połączone z rekordem pliku, z którego zostały wyodrębnione. MUSI być możliwe wstępne przeglądanie wyniku analizy (preview) w postaci tekstu lub HTML.
98. Rozwiązanie MUSI umożliwiać operatorowi edycję dostępnych pól bezpośrednio w interfejsie WebUI zgodnie z przydzielonymi uprawnieniami. Uprawnienia MUSZĄ być konfigurowalne indywidualnie dla każdego pola. Minimalny zakres uprawnień to: brak, odczyt, odczyt-zapis. Zmiany w polach MUSZĄ być widoczne w logu audytowym systemu.
99. Playbook-i MUSZĄ być pogrupowane w foldery z możliwością eksportowania lub importowania całego folderu bezpośrednio z WebUI. Dzięki temu możliwa będzie migracja schematów pomiędzy systemem testowym a produkcyjnym.
100. Playbook-i MUSZĄ mieć co najmniej 3 priorytety wykonywania, pozwalające na wykonanie niektórych przed innymi w kolejce w zależności od ich ważności.
101. Playbook-i MUSZĄ mieć wyzwalanie warunkowe. Nie będą się uruchamiać, chyba że spełnione są określone warunki. Poniższe operatory warunków muszą być obsługiwane:
    a) równy
    b) nie równa się
    c) mniej niż/mniej niż lub równa się
    d) większe niż/większe niż lub równe
    e) jest na liście

f) nie ma na liście
g) pusty
h) jest zgodny z zadanym wzorcem (pattern)
i) nie jest zgodny z zadanym wzorcem (pattern)
j) Warunki MUSZĄ obsługiwać sumę logiczną (dowolny warunek spełniony) oraz iloczyn logiczny (wszystkie warunki muszą być spełnione).

102. Playbook-i MUSZĄ mieć co najmniej 3 priorytety wykonywania, pozwalające na wykonanie niektórych przed innymi w kolejce w zależności od ich ważności.
103. Playbook-i MUSZĄ obsługiwać następujące sposoby uruchomienia:
    a) analityk może ręcznie uruchomić w GUI systemowym
    b) automatycznie przy zmianie rekordu (Alert, wskaźnik, incydent... itd.): utworzony/zmieniony/usunięty
    c) przez API: gdy SOAR otrzymał żądanie API z określonymi parametrami to uruchamia określonego Playbook-a
    d) referencja: playbook ma możliwość wykonania innego playbook-a z zadanymi parametrami
104. System MUSI zapewniać graficzny edytor Playbook-ów, w którym użytkownicy mogą używać myszy do przeciągania i upuszczania operacji lub kolejnych kroków. Ponadto edytor playbook MUSI zawierać panele pomocnicze do pobierania wszystkich dostępnych zmiennych, wybierania wszystkich typów operacji, tworzenia wyrażeń złożonych. Tworzenie Playbook-a lub jego edycja NIE MOŻE wymagać uruchamiania jakiegokolwiek innego interfejsu.
105. Graficzny edytor Playbook-ów MUSI mieć możliwość cofania kroków edycji jak i ich ponawiania. Przykładowo możliwe jest przywrócenie wcześniej usuniętej operacji.
106. Rozwiązanie MUSI umożliwiać użytkownikowi uruchomienie Playbook-a z poziomu edytora graficznego i przetestowanie jego wykonania ze zmiennymi wybranego rekordu istniejącego w systemie lub ostatnim rekordem, z którym Playbook został wykonany.
107. Administratorzy muszą mieć możliwość indywidualnego eksportowania i importowania Playbook-ów, w tym dowolnie wybranej wersji (podobnie jak SVN / GIT).
108. Rozwiązanie MUSI obsługiwać tworzenie, modyfikowanie i usuwanie zmiennych globalnych dostępnych dla wszystkich Playbook-ów. Zmienne globalne muszą być edytowalne za pomocą Playbook-ów lub GUI.
109. System MUSI dostarczyć wizualną historię wykonania Playbook-ów, która identyfikuje dane wyjściowe, wejściowe i konfigurację każdego kroku.
110. Poziom logowania wykonywania Playbook-ów MUSI być konfigurowalny zarówno globalnie (w całym systemie) jak i lokalnie dla każdego Playbook-a indywidualnie. Muszą być wspierane co najmniej dwa poziomy logowania: informacyjny i debug.
111. Narzędzia do debugowania muszą być dostępne z poziomu edytora Playbook-ów. Debugger MUSI być w stanie korzystać z danych z poprzedniego wykonania Playbook-a lub danych dostarczonych przez analityka.
112. Kontrola praw dostępu (RBAC) MUSI obejmować Playbook-i w zakresie zapisu i uruchamiania.
113. Rozwiązanie MUSI zawierać szczegółowe komunikaty o błędach, gdy wykonanie Playbook - a nie powiedzie się i zezwalać na ponowne uruchomienie Playbook-a od kroku, w którym wykonanie nie powiodło się.
114. Kroki warunkowe w wykonywaniu Playbook-ów muszą być wystarczająco elastyczne, aby móc stosować złożone warunki. Wymagane możliwości budowania warunków:
    a) równy - porównuje dwa obiekty i wykonuje operację, gdy równe
    b) nierówna się - porównuje dwa obiekty i wykonuje operację, gdy nie równe
    c) większy niż - prawda, jeśli lewa strona jest większa niż prawa strona
    d) większy niż lub równy - prawda, jeśli lewa strona jest większa lub równa prawej stronie
    e) mniejsze niż - prawda, jeśli lewa strona jest mniejsza niż prawa strona
    f) mniejsze lub równe - prawda, jeśli lewa strona jest mniejsza lub równa prawej stronie
    g) i - zwróć wartość „prawda”, jeśli lewe i prawe wyrażenie są prawdziwe
    h) lub - zwróć wartość „prawda”, jeśli lewe lub prawe wyraże nie jest prawdziwe
    i) nie – negacja
    j) dodawanie - dodaje do siebie dwa obiekty
    k) odejmowanie - odejmij drugą liczbę od pierwszej
    l) dzielenie - dzielenie dwóch liczb
    m) modulo - obliczanie reszty z dzielenia liczby całkowitej
    n) mnożenie - mnożenie dwóch wartości
    o) potęga - podnieś lewy operand do potęgi prawego operandu

    Warunki takie jak:
    (zmienna_X + zmienna_Y)/2 > 3
    ((zmienna_X + zmienna_Y)/2 >zmienna_Z) OR (zmienna_A / zmienna_B) < 2
    muszą być możliwe bez użycia języka programowania .Etap podejmowania decyzji MUSI mieć opcję ustawienia domyślnego następnego kroku, jeśli wszystkie warunki zawiodą.

115. Operatorzy muszą mieć możliwość zastosowania języka programowania, co najmniej Python bezpośrednio w Playbook-ach. Administrator SOAR MUSI być w stanie ograniczyć dostęp i możliwość wykorzystania bibliotek języka Python (z dokładnością do pojedynczych bibliotek).
116. Kroki Playbook-ów muszą być konfigurowalne na wypadek wystąpienia błędu. Jeśli wystąpi błąd na poziomie kroku to MUSI być możliwy wybór co najmniej przekazania komunikatu o błędzie do następnego kroku i kontynuowanie lub zaprzestanie dalszego wykonywania.
117. Zarządzanie Playbook-ami MUSI umożliwiać analitykom zbiorczą ich edycję z możliwością wykonywania poniższych funkcji:
    a) Zmiana statusu (Playbook aktywny lub nieaktywowany)
    b) Klonowanie wybranych Playbook-ów
    c) Przenoszenie wybranych Playbook-ów do innej grupy
    d) Zmiana poziomu logowania dla wybranych Playbook-ów
    e) Eksportowanie wybranych Playbook-ów
118. Każdy Playbook w ramach proponowanego rozwiązania MUSI mieć możliwość automatycznego uruchomienia w określonych odstępach czasu z możliwością zapobieżenia jego wykonaniu, jeśli poprzednie wystąpienie jest nadal uruchomione.
119. W ramach edytora Playbook-ów analitycy muszą być w stanie wykonać operacje:
    a) sklonuj krok
    b) kopiuj i wklej krok lub grupę kroków do tego samego Playbook-a lub innego
    c) wyrównaj wizualnie kroki na diagramie do układu pionowego lub poziomego - wybierz krok lub grupę kroków i usuń je
120. Playbook-i MUSZĄ mieć możliwość wykonania kroku, gdzie konfigurowalne będzie uzyskanie danych i/lub potwierdzenia za pośrednictwem wiadomości e-mail zawierającej link do decyzji z opcją podjęcia określonej akcji w przypadku przekroczenia limitu czasu. Przykładem może być wysłanie wiadomości z prośbą o zgodę na restart urządzenia wraz z informacją zwrotną o dogodnym terminie.
121. System MUSI zapewniać przyjazny dla użytkownika kreator pozyskiwania danych zewnętrznych (np. informacje o użytkownikach, podatnościach) w celu stworzenia mechanizmu integracji pozwalającego na ciągłe i automatyczne pobieranie wymaganych informacji.
122. System MUSI zapewnić pulpit (dashboard) z informacją o kondycji konektorów, który wskazuje, czy wszystkie integracje z systemami zewnętrznymi działają prawidłowo.
123. Akcje konektorów muszą podlegać prawom dostępu RBAC tak aby tylko zdefiniowane role mogły używać zdefiniowanych akcji z dokładnością do pojedynczej akcji.
124. System MUSI umożliwiać analitykowi uruchamianie dowolnej akcji konektora do której ma prawo, za pośrednictwem interfejsu GUI bez użycia Playbook-a.
125. Musi istnieć możliwość zbiorczego importu i eksportu wskaźników IOC bezpośrednio z GUI.
126. Rozwiązanie MUSI być na tyle elastyczne, aby umożliwić generowanie reputacji wskaźników na podstawie danych z różnych źródeł Threat Intelligence jednocześnie.
127. Rozwiązanie MUSI umożliwiać tworzenie kopii zapasowych i przywracanie zarówno konfiguracji systemu, jak i zebranych danych.
128. Rozwiązanie MUSI mieć możliwość tworzenia niestandardowych modułów funkcjonalnych z poziomu interfejsu GUI. Moduł jest podsystemem do zarządzania nowym typem rekordów, takich jak: Alerty, Incydenty, wskaźniki, itp.
129. Architektura systemu MUSI pozwalać na skalowanie rozwiązania jak i tworzenie wysokiej dostępności. Musi istnieć możliwość klastrowania wielu węzłów (minimum 3) w konfiguracji Aktywny/Aktywny.
130. Rozwiązanie MUSI oferować skalowalną geograficznie, rozproszoną architekturę z możliwością separacji części zasobów dla podległych jednostek lub innych użytkowników (model pracy MSSP).
131. Rozwiązanie MUSI umożliwiać uruchamianie Playbook-ów i kolekcję danych w zdalnych segmentach sieci za pośrednictwem agenta SOAR wdrożonego w segmencie sieci zdalnej. Agenty muszą obsługiwać automatyczne aktualizacje.
132. System MUSI umożliwiać korzystanie zarówno z wewnętrznej, jak i zewnętrznej bazy danych.
133. Rozwiązanie MUSI oferować aplikację mobilną co najmniej dla systemu Android do zdalnego zarządzania i monitorowania w ramach SOAR.
134. System MUSI zapewniać globalne logowanie aktywności (audyt) obejmujące zarówno działania użytkowników (takie jak logowanie, wylogowanie, instalacje, itp.) jak i zdarzenia związane z danymi (np tworzenie rekordów, aktualizowanie, usuwanie…)
135. System MUSI mieć możliwość przesyłania zdarzeń audytu i aplikacji do serwera zewnętrznego lub rozwiązania SIEM. Następujące protokoły muszą być obsługiwane z konfigurowalnym poziomem dziennika:
    a) UDP
    b) TCP, TCP/TLS
    c) RELP, RELP/TLS

136. System MUSI posiadać skonfigurowany widżet osi czasu dziennika inspekcji śledzący każde zdarzenie dla rekordu w alarmach, incydentach ze szczegółami każdej zmiany. Przykłady: uruchomienie Playbook-a, dodanie komentarza, zmiana wartości, etc.
137. System MUSI zapewniać szczegółową i elastyczną kontrolę dostępu opartą na rolach (RBAC). Administratorzy muszą mieć możliwość ustawienia praw dostępu dla każdego typu rekordu do poziomu pola. Na przykład pole „źródłowy adres IP".
138. SOAR MUSI obsługiwać hierarchię grup użytkowników. Grupa MUSI mieć możliwość dziedziczenia zakresu dostępu z innej grupy lub grup według poziomów: grupa nadrzędna (parent) – ma dostęp do danych niższych grup i swojej
    a) grupa równoważna (sibling) – ma dostęp do danych grup w ramach ustawionego połączenia
    b) grupa podrzędna (child) – brak możliwości dostępu do danych z nadrzędnych grup
139. System powinien zapewniać wiele konfigurowalnych pulpitów nawigacyjnych (dashboard), które działają zgodnie z prawami dostępu RBAC.
140. System powinien zapewniać mechanizm wyróżniania alertów, które zbliżają się do naruszeń SLA.
141. Pulpit nawigacyjny powinien móc wyświetlać informacje specyficzne dla analityka, takie jak alerty i zadania przypisane do niego.
142. SOAR powinien obliczać szacowany zwrot z inwestycji i wyświetlenie go na pulpicie (dashboard).
143. Powinno być możliwe importowanie i eksportowanie szablonów pulpitu nawigacyjnego.
144. System powinien posiadać skonfigurowane pulpity nawigacyjne dedykowane dla ról, takich jak: analityk linii 1, analityk linii 2, menedżer SOC.
145. SOAR MUSI mierzyć wskaźniki SOC dla incydentów, takie jak średni czas dla poszczególnych faz ataku wg. killchain. Powinno być możliwe wyświetlanie tych danych na pulpicie nawigacyjnym.
146. Rozwiązanie MUSI mieć dedykowany pulpit nawigacyjny do monitorowania stanu/dostępności każdej integracji, a także kondycji systemu SOAR.
147. Rozwiązanie MUSI obsługiwać dostosowanie znaków graficznych (branding) interfejsu użytkownika dla różnych domen MSSP.
148. Rozwiązanie MUSI zapewniać framework dla przygotowana własnego pulpitu nawigacyjnego zgodny z HTML/JSON/JS, aby umożliwić tworzenie niestandardowych widżetów pulpitu nawigacyjnego i importowanie ich do rozwiązania SOAR.
149. System MUSI zapewniać konfigurowany moduł raportowania w GUI.
150. Raporty MUSZĄ mieć możliwość zaplanowania uruchamiania w czasie zdefiniowanym przez użytkownika.
151. Raporty MUSZĄ być generowane w co najmniej formatach CSV i PDF.
152. Wygenerowane raporty MUSZĄ mieć opcję wysłania pocztą elektroniczną.
153. MUSI być możliwe uruchamianie raportów z poziomu playbook.
154. Dostęp do raportów MUSI być ograniczany prawami dostępu RBAC.
155. System MUSI posiadać logi audytu, które dostarczą informacji o aktywności modułu raportowego, włączając akcję pobrania raportu.
156. MUSI istnieć możliwość dołączania do raportu grafik i wykresów.
157. System MUSI posiadać moduł zarządzania zmianą operatorów, w szczególności MUSZĄ być obsługiwane funkcje:
    a) generowanie kalendarza zmiany wg założonego wzoru, np. 8 godzin od 6:00 na tydzień do przodu, dni robocze dla wybranych użytkowników
    b) przekazywanie zmiany: przydzielanie niezamkniętych dochodzeń zmiany kończącej do zmiany rozpoczynającej pracę
    c) przypisywanie musi być możliwe dla wszystkich niezamkniętych spraw, które rozpoczęły się w zadanym przedziale czasu, np. ostatnie 7 dni
    d) przypisywane rekordy muszą mieć możliwość filtrowania:
        a. filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne)
        b. poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione)
    e) musi być możliwe przypisanie rekordu:
        a. nie przypisany
        b. przypisany kierownikowi zmiany
        c. wg. metody round robin w ramach członków zmiany
158. System MUSI posiadać moduł zarządzania kolejkami nadchodzących zdarzeń. Domyślnie musi być możliwe tworzenie dedykowanych kolejek dla rekordów typu zadanie, alarm i incydent. Każda kolejka musi się charakteryzować funkcjami co najmniej:
    a) wybór typu rekordu – dowolny zestaw (jeden typ, wszystkie typy)
    b) musi być możliwe dodawanie nowych typów rekordów do kolejek
    c) kolejka musi obsługiwać filtry wejściowe dla rekordów, minimalny zakres to:

a. utworzenie lub aktualizacja rekordu
b. filtrowanie na podstawie zawartości pól charakterystycznych rekordu i operacje na nich (zawiera, nie zawiera, istnieje, nie istnieje, jest na liście, spełnia wyrażenie regularne
c. poszczególne filtry podlegają sumie logicznej (dowolny spełniony) lub iloczynowi logicznemu (wszystkie spełnione)

d) musi być możliwe ustawienie priorytetu rekordu w ramach kolei
e) musi być możliwe przypisanie rekordu:
a. nie przypisany
b. przypisany kierownikowi grupy
c. wg. metody roundrobin w ramach członków grupy

159. System SOAR musi być zaoferowany łącznie z integracją z systemami wymienionymi w Załączniku do wymiarowania SOAR. Należy jasno zaznaczyć integracje istniejące i udokumentowane w rozwiązaniu na dzień składania oferty.
160. System SOAR powinien posiadać gotowe integracje w postaci konektorów i akcji wraz z przykładowymi Playbooka-mi. Na dzień złożenia oferty należy przedstawić ilość gotowych i udokumentowanych integracji. Integracje te muszą być widoczne w oficjalnej dokumentacji produktu, dostępnej publicznie bez konieczności logowania lub uzyskiwania dostępu.
161. Wymaga się, aby oferowany system miał co najmniej 500 gotowych integracji.

XI. MINIMALNE WYMAGANIA W ZAKRESIE LICENCJI OPROGRAMOWANIA SOAR

1. Dostarczony system SOAR musi spełniać następujące wymagania licencyjne:
2. Licencja musi być dostarczona w formie licencji na wieczyste użytkowanie (ang: perpetual) z gwarancją i wsparciem producenta na okres wskazany w formularzu technicznym od daty końcowego odbioru
3. Licencja nie może w żaden sposób ograniczać ilości wykonywanych akcji przez system, ilości integracji, rozmiaru dysku, skonfigurowanych kont użytkowników.
4. System nie może ograniczać ilości skonfigurowanych kont operatorów lub administratorów.

XII. MINIMALNE WYMAGANIA W ZAKRESIE INTEGRACJI SYSTEMÓW SIEM i SOAR

1. Wymaga się, aby oferowane systemy SIEM i SOAR w pełni ze sobą współpracowały. Minimalny zakres integracji to:
   a) Automatyczne pobieranie alarmów z SIEM do SOAR i ich wzbogacanie
   b) Zamykanie alarmów w SIEM w momencie zakończenia obsługi problemu w systemie SOAR wraz z opisem oraz powodem zamknięcia
   c) Uruchomienie akcji konektora w SOAR z poziomu GUI SIEM
   d) Uruchomienie procedury (playbook) w SOAR z poziomu GUI SIEM
   e) Wykonywanie wyszukiwań i raportów z poziomu SOAR w SIEM
   f) Zarządzanie listami referencyjnymi w SIEM za pomocą SOAR

XIII. MINIMALNE WYMAGANIA w ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z PRZEPROWADZENIEM INSTRUKTAŻU

1. Dostarczenie i instalacja platformy wirtualizacji będzie realizowana we wskazanej lokalizacji przez Zamawiającego Sprzęt będący przedmiotem niniejszego zamówienia zostanie dostarczony do lokalizacji wskazanej przez Zamawiającego.
2. Dostarczenie platformy obejmuje dostawę wszelkich wymaganych do działania platformy oprogramowania oraz licencji/subskrypcji.
3. Konfigurację i uruchomienie urządzeń/elementów platformy wirtualizującej w środowisku Zamawiającego w terminie do 60 dni od podpisania umowy.
4. Wykonawca przeprowadzi instalację i konfigurację wszystkich elementów dostarczonego systemu wymaganą przez Zamawiającego.
5. Wszelkie prace konfiguracyjne muszą uwzględniać dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta dostarczonej infrastruktury sprzętowej oraz programowej.
6. Wdrożony klaster wirtualizacyjny musi być skonfigurowany tak, aby był w pełni funkcjonalny we wszystkich czterech aspektach: serwerowym, dyskowym, sieciowym i zarządzania.
7. Przed rozpoczęciem prac należy ustalić plan adresacji sieci IP. Ustalenia te będą prowadzone z wyznaczonym do tego celu pracownikiem/pracownikami Zamawiającego.
8. Zamawiający zapewni przestrzeń min. 15U w szafie RACK 19”, zasilanie gwarantowane wraz z niezbędną ilością gniazd w listwach zasilających.
9. Zamawiający zapewni niezbędną ilość portów w standardzie 1000BASE-T na potrzeby zarządzania dostarczonym środowiskiem.

10. Prace wdrożeniowe klastra wirtualizacyjnego będą polegały w szczególności na:
    a. montażu i podłączeniu fizycznym sprzętu w serwerowni (szafa RACK wskazana przez Zamawiającego),
    b. podłączeniu zasilania oraz sieci management,
    c. aktualizacji oprogramowania układowego i jego komponentów wszystkich serwerów, macierzy, przełączników sieciowych oraz FC do wersji rekomendowanych przez producenta,
    d. konfiguracji przełączników FC, macierzy dyskowej, przełączników sieciowych,
    e. konfiguracji systemu backupu Zamawiającego
    f. hardeningu urządzeń oraz wdrażanego oprogramowania według najlepszych praktyk producenta,
    g. niezbędnej rekonfiguracji istniejącej infrastruktury informatycznej (VLANY, routing, polityki firewalla, wpisy DNS),
    h. aktywacji zakupionego oprogramowania oraz wszelkich subskrypcji i serwisów producenta,
    i. konfiguracji oraz uruchomieniu klastra wirtualizacyjnego, opartego o dostarczane oprogramowanie witrualizacyjne.

11. Prace wdrożeniowe dla systemów SIEM oraz SOAR będą polegały w szczególności na:
    a. Analizie i wykonaniu Projektu Technicznego
    b. Instalacji i konfiguracji oprogramowania SIEM i SOAR według najlepszych praktyk producenta
    c. Konfiguracji autentykacji i autoryzacji do systemów włączając w to integrację z usługami zarządzania tożsamością działających u Zamawiającego
    d. Konfiguracji integracji z Threat Intelligence
    e. Przeprowadzeniu pełnej integracji wskazanych przez Zamawiającego 5 systemów źródłowych z SIEM w celu zapewnienia kompletnego przepływu logów ze wszystkich istotnych elementów infrastruktury IT.
    f. Skonfigurowaniu procesów normalizacji i parsowania danych, aby wszystkie logi były ujednolicone i gotowe do skutecznej analizy.
    g. Utworzeniu reguł korelacyjnych pozwalających na wykrywanie zaawansowanych scenariuszy ataków i nietypowych aktywności w środowisku.
    h. Przygotowaniu spersonalizowanych dashboardów i raportów, które umożliwią zespołowi SOC szybkie monitorowanie stanu bezpieczeństwa.
    i. Zdefiniowaniu przypadków użycia wraz z ich mapowaniem do standardów takich jak MITRE ATT&CK lub NIST w celu ujednolicenia monitoringu zagrożeń.
    j. Zrealizowaniu integracji SOAR z narzędziami zabezpieczeń, systemami ticketowymi, platformami skanowania i urządzeniami sieciowymi w celu umożliwienia automatycznych reakcji.
    k. Opracowaniu i wdrożeniu 10 playbooków automatyzacji reakcji na incydenty, obejmujących zarówno działania automatyczne, jak i półautomatyczne.
    l. Wykonaniu testów wydajności, bezpieczeństwa oraz procedur odtwarzania po awarii w celu potwierdzenia gotowości systemów do pracy w środowisku produkcyjnym.
    m. Przygotowaniu dokumentacji zawierającej
        i. Informacje o architekturze i konfiguracji systemu
        ii. procedurę aktualizacji systemu.
        iii. Procedury utrzymaniowe związane z cyklicznymi czynnościami administracyjnymi. Najlepsze praktyki.
        iv. Procedura integracji z systemami trzecimi
        v. Procedura podłączania źródeł via agent systemu

12. Wykonaniu testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowaniu i przedstawieniu Raportu z testów. Wykonanie dokumentacji powykonawczej wszystkich wdrożonych elementów.

13. Dokumentacja powykonawcza, musi w szczególności zawierać następujące elementy:
    a. architektury logicznej,
    b. architektury fizycznej,
    c. architektury sieciowej,
    d. konfiguracji klastra wirtualizacyjnego, zasobów dyskowych i sieci,
    e. zestawienie wersji firmware zainstalowanych na dostarczonych urządzeniach,
    f. zestawienie zakupionego i aktywowanego oprogramowania,
    g. specyfikacja techniczna dostarczonego sprzętu,
    h. schemat rozmieszczenia zainstalowanych urządzeń w szafach RACK i fizycznymi połączeniami między nimi,
    i. tabele wykorzystanych adresów IP

j. zebrane informacje na temat obsługi wsparcia dostarczonych urządzeń, adresy url, nazwy kont do logowania, numery telefonów, adresy e-mail

14. Przeprowadzenie warsztatów autorskich z poniższych zakresów
    a. administracja systemem
    b. Obsługi incydentów
    c. Budowy korelacji
    d. Budowy monitoringu i obsługi bazy CMDB

15. Wykonawca przeprowadzi instruktaż dla administratorów wskazanych przez Zamawiającego:
    a) Instruktaż zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż 10 dni od daty wdrożenia), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa.
    Instruktaż powinien obejmować:
    b) omówienie dostarczonego sprzętu i oprogramowania (parametry, funkcjonalności),
    c) omówienie przeprowadzonych prac instalacyjno-konfiguracyjnych,
    d) omówienie i weryfikację przygotowanych i dostarczonych procedur,
    e) omówienie scenariuszy w przypadku wystąpienia błędów/awarii.

    Przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/programu instruktażu. Zamawiający będzie miał prawo do weryfikacji zakresu tematycznego/programu instruktażu i zgłoszenia ew. dodatkowego zakresu tematycznego.

XIV. MINIMALNE WYMAGANIA W ZAKRESIE ASYSTY TECHNICZNEJ

1. Wykonawca przez cały okres trwania umowy zobowiązany będzie do świadczenia usługi asysty technicznej na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego.
2. Zakres, sposób oraz termin realizacji zostanie uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3. Zlecenia będą obejmować w szczególności:
    1) Zapewnieniu Zamawiającemu pomocy w rozwiązaniu problemów i incydentów wynikłych w trakcie obsługi dostarczonego sprzętu oraz oprogramowania tj.:
        a. analiza problemów zgłaszanych przez Zamawiającego,
        b. asysta przy określaniu i usuwaniu przyczyn oraz skutków zgłaszanych incydentów,
        c. dostarczanie, instalacja (po uzyskaniu zgody Zamawiającego) i konfiguracja uaktualnień i nowych wersji oprogramowania lub jego komponentów, oraz związana z tym aktualizacja dostarczonej dokumentacji,
        d. przeprowadzanie analiz oraz udzielanie konsultacji Zamawiającemu,
        e. dokonywanie zmian konfiguracji oprogramowania,
        f. opracowywanie i dostarczanie dokumentacji, w tym aktualizacji dokumentacji oraz dostarczanie dokumentacji wprowadzanych zmian.
        g. implementację nowych funkcjonalności lub modyfikację już skonfigurowanych.
    2) Wsparcie w przypadku wystąpienia incydentu bezpieczeństwa.
        a. Wsparcie w zakresie wykonania analizy wykorzystanych podatności.
        b. Kontaktu z ekspertem w zakresie bezpieczeństwa dostarczonego systemu.
        c. Analizy zakresu kompromitacji systemu.
        d. Wsparcia w konfiguracji/rekomendacji w celu zabezpieczenia systemu,
        e. Wsparcia w zakresie usunięcia skutków oraz rozwiązania incydentu bezpieczeństwa,
    3) Wsparcie w planowanych pracach serwisowych,
        a. Przeprowadzenia standardowych prac serwisowych,
        b. Przeprowadzania aktualizacji komponentów systemu,
        c. Weryfikacji poprawności konfiguracji,
        d. Zmiany w topologii sieci,
        e. Wsparcia w okresie podwyższonej czujności (np. Monitoring środowiska w czasie biznesowo krytycznych wydarzeń),
    4) Wsparcie on-site w przypadku braku możliwości rozwiązania problemu zdalnie.
    5) usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.
4. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
    a) w siedzibie Zamawiającego przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług,

uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez liczbę godzin wskazanych w zleceniu,

b) zdalnie przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez określoną liczbę godzin w danym dniu. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.

5. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
6. Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.
7. Zamawiający zastrzega sobie prawo do nie udzielania zleceń na usługi asysty technicznej.
8. Proces realizacji asysty technicznej będzie przebiegał następująco:
   a) Zamawiający przekaże Wykonawcy drogą mailową zakres oczekiwanej usługi asysty oraz oczekiwany termin realizacji.
   b) W terminie nie dłuższym niż 3 dni robocze od dnia otrzymania przez Wykonawcę zakresu asysty technicznej, Wykonawca przekaże Zamawiającemu wycenę pracochłonności wyrażoną w roboczogodzinach oraz wskazująca termin realizacji.
   c) Wykonawca przystępuje do realizacji zlecenia po otrzymaniu od Zmawiającego zlecenia realizacji usługi asysty technicznej.

XV. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI

Gwarancja dla oferowanych urządzeń i oprogramowania musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na urządzenia i oprogramowanie wskazany w Formularzu Ofertowym
2. Zamawiający wymaga, aby usługa gwarancyjna na wszystkie dostarczone w ramach zamówienia Sprzęty była, przez cały okres jej trwania, świadczona na podstawie wykupionego wsparcia producenta dostarczonych urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczanego urządzeń i był jego autoryzowanym dostawcą.
3. Wszystkie urządzenia dostarczone i zastosowane przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem producenta Urządzeń lub jego polskiego przedstawicielstwa, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu najpóźniej w dniu dostawy oferowanych Urządzeń.
4. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producentów rozwiązania. Serwis gwarancyjny świadczony ma być w miejscu instalacji Sprzętów.
5. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
6. Zamawiający dopuszcza świadczenie serwisu dla dostarczonych urządzeń poprzez zastosowanie zamienników wskazanych przez producenta tylko i wyłącznie w przypadku, gdy takiego wsparcia u producenta nie da się wykupić (np. produkty zostały wycofane przez producenta bez możliwości świadczenia serwisu).
7. W przypadku, gdy w okresie gwarancyjnym nastąpi trzykrotna naprawa wadliwego podzespołu Wykonawca niezwłocznie tj. w terminie nie dłuższym niż 14 dni liczonych od dnia zgłoszenia awarii, dokona jego wymiany na sprzęt nowy, wolny od wad. Na czas potrzebny do wymiany podzespołu wykonawca dostarczy element zastępczy o parametrach tożsamych z podzespołem uszkodzonym. Zamawiający oczekuje, iż w wypadku konieczności wymiany urządzenia, dyski na których zapisane są dane nieulotne wymienianego urządzenia pozostaną w siedzibie Zamawiającego.
8. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń w godzinach pracy Zamawiającego.
9. Zamawiający zastrzega sobie prawo do dodawania nowych modułów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą. W przypadku nieprawidłowego lub niezgodnego z zaleceniami Wykonawcy i

producenta Urządzenia dodania modułów lub wymiany zainstalowanych modułów przez Zamawiającego Wykonawca nie jest obciążony gwarancją i rękojmią w tym zakresie.

10. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware) oraz patche i programy korekcji błędów, a także dostęp do usług wsparcia technicznego producenta właściwy dla danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu ww. przed podpisaniem protokołu odbioru Urządzeń.
11. W przypadku konieczności naprawy Urządzenia lub Oprogramowania poza Lokalizacją, Wykonawca pokrywa koszty transportu i ponosi ryzyko uszkodzenia lub przypadkowej utraty urządzenia lub oprogramowania Standardowego w przypadku konieczności naprawy poza siedzibą Zamawiającego.
12. Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowe od chwili zgłoszenia awarii.
13. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej prac rezerwowego Urządzenia i/lub procedur zastępczych.
14. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
15. W ramach gwarancji Zamawiający będzie miał prawo przez okres wskazany w formularzu ofertowym do:
    a) pobierania i instalowania nowych wersji oprogramowania dla każdego elementu wchodzącego w skład oferty
    b) Dostępu do bazy wiedzy oraz dokumentacji dostarczonych elementów
    c) Dostępu do powiadomień/ogłoszeń/alarmów w zakresie dostarczonych elementów
    d) Zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego,
    e) Wymiany uszkodzonych/wadliwych dostarczonych elementów w trybie NDB (Next-Bussines Day),
16. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:
    a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,
    b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,
    c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,
    d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.
17. Wykonawca do dostarczonych urządzeń, będących przedmiotem zamówienia, dołączy karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
18. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.
19. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych.
20. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie urządzeń i oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia urządzeń i oprogramowania powstałych z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.
21. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego

zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-17:00.

22. W ramach gwarancji Wykonawca zobowiązany będzie do dokonywania okresowych (nie rzadziej niż co 6 m-cy) przeglądów gwarancyjnych dostarczonego oprogramowania. W ramach przeprowadzanych okresowych przeglądów gwarancyjnych muszą być wykonane co najmniej następujące czynności:
    a) weryfikacja poprawności działania oraz optymalizacja konfiguracji wszystkich komponentów wchodzących w skład dostarczonego rozwiązania,
    b) analiza logów i podjęcie działań naprawczych w razie potrzeby,
    c) aktualizacja (w razie potrzeby i po uzyskaniu uprzedniej zgody Zamawiającego) wersji poszczególnych komponentów wchodzących w skład dostarczonego rozwiązania.
23. Zamawiający wymaga obsługi zgłoszeń w języku polskim.