IIiGG.271.8.2025

zał. nr 2 do Zapytania ofertowego

Szczegółowy opis przedmiotu zamówienia

I. Uwagi ogólne:

Niniejszy dokument prócz zdefiniowania minimalnych wymagań dotyczących przedmiotu zamówienia, będzie potwierdzał, ze oferowany sprzęt i oprogramowanie spełnia wymogi zapytania ofertowego. W związku z powyższym Wykonawca zobowiązany jest do dokonania szczegółowej analizy załącznika pod kątem sformułowanych wymogów i wypełnienie stosownych kolumn tabel ujętych w części II i III załącznika **(wymóg nie dotyczy: cz. 6 Usługa konfiguracyjna pozwalająca wdrożyć nowe rozwiązania informatyczne, gdzie Wykonawca zobowiązany jest jedynie potwierdzić realizację przedmiotowego zakresu w ramach złażonej oferty w cz. II i III załącznika wybierając odpowiednią opcję)**. Następnie Wykonawca zobowiązany jest do dołączenia wypełnionego dokumentu do złożonej oferty.

W części II Wykonawca zobowiązany jest do podania oferowanego modelu lub wersji oraz producenta oferowanego asortymentu (w kolumnie 3).

W części III natomiast Wykonawca zobowiązany jest do odniesienia się do opisanego wymogu i wpisanie danych (w kolumnie 3), które będą miały za zadanie jednoznaczne potwierdzenie spełnienie danego wymogu. Wpisy ogólne typu: „zgodne z zapytaniem” nie będą traktowane przez Zamawiającego jako prawidłowe.

Zamówione urządzenia i oprogramowanie, mają być fabrycznie nowe, kompletne, nieużywane i pozbawione wad fizycznych i prawnych. Zamawiający wyklucza dostawę sprzętu używanego, poleasingowego, powystawowego, po zwrocie itp. Nie dopuszcza się zaoferowania sprzętu refurbished. Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający. Zamawiający nie dopuszcza stosowania licencji używanej, przeniesionej z innego sprzętu oraz licencji typu refurbished. Nie dopuszcza się stosowania adapterów, przejściówek, ani innych urządzeń zewnętrznych w celu osiągnięcia wymaganych portów i funkcjonalności urządzeń. Wyjątek stanowi sytuacja, że dopuszczenie adapterów jest wyraźnie opisane w opisie pozycji przedmiotu zamówienia.

Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

II. Zestawienie Oferowanego sprzętu, oprogramowania lub usług:

Lp.	Przedmiot zamówienia	Producent/ Model/Wersja
1	*2*	*3*
1.	**Oprogramowanie: Zakup systemu monitorowania sieci i użytkowników 30 USER (SIEM)**	
2.	**Serwer z macierzą dyskową SSD 1 szt.**	
3.	**UPS typ 1 -1 szt.**	
4.	**Przełącznik 1 szt.**	
5.	**UPS typ 2 - 5 szt.**	
6.	**Usługa konfiguracyjna pozwalająca wdrożyć nowe rozwiązania informatyczne.**	**TAK/NIE***

**Wybrać odpowiednie.*

1. Oprogramowanie: Zakup systemu monitorowania sieci i użytkowników 30 USER (SIEM)

Nazwa parametru lub wymaganej funkcjonalności	Charakterystyka (wymagania minimalne)	Opis oferowanej funkcjonalności lub parametru
1	*2*	*3*
LICENCJA	● W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową. ● Oprogramowanie musi posiadać wsparcie min. do dnia 25-05-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta. ● Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej. ● Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych	
WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA	Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci. Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.	

	Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców. Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności). Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów. Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów. Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania. Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT. Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych	

	ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje. Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych. Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie). Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych. Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów. Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS. Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA. Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami. Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie. Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie. Zgodność ze standardami HTML i CSS całego serwisu www.	

	Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA. System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.	
Wymagania budowy systemu	System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły	
MODUŁ ANALIZY PODATNOŚCI	1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania. System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji. Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności “nowe”, których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor. 1.2. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.	

	System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji. 1.3. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT. System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).	
MODUŁ MONITORINGU ZASOBÓW	2.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.) System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system	

	musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny). 2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy. 2.3. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.	

	2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko “nowe” problemy i zdarzenia oraz te, których status nie został zmieniony na “rozwiązany” bądź “anulowany”. Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, system przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: “help-desk”, przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie. 2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej	

	Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany). 2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu. 2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w	

	systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu. 2.8 Zdalny dostęp do urządzeń końcowych System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH. 2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim. 2.10 Analiza ruchu sieciowego System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach	

	informatycznych. Użytkownik systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM. 2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.	
MODUŁ ANALIZY LOGÓW	3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn. Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych. 3.2. Możliwość analizy tzw. „customowych” logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych. System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw.	

	"customowych" logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system. 3.3. Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu. Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzinowego - "customlogów"), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji. 3.4. Przegląd i analiza logów dotyczących działań użytkowników. W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie. 3.6. Dostęp do logów historycznych.	

	System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie. 3.7. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej. System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log “customowy”). Ponadto CSB musi informować użytkownika/administratora o “nowych” zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a “nowe” logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora. 3.8. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd). System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb	

	użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).	
MODUŁ EDR/XDR	4.1 System musi posiadać własny moduł EDR/XDR, czyli zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach. 4.2 Moduł posiadać podgląd informacji, alertów i zdarzeń występujących w środowisku IT. W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet. 4.3 Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender). System musi umożliwiać bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.	

MODUŁ INWENTARYZACJI	5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej. System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez "ręczne" wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB. 5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja) Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu "ręcznym" system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości. 5.3. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.	

	Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.	
MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)	6.1. Integracja z systemem tiketowym. System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu. 6.2. Zgłaszanie incydentu/problemu, który został namierzony przez system. Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na	

	urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku "Zgłoś Problem". Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu. 6.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK. System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.	
MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)	7.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK. System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.	

	7.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny. 7.3. Historia wykrytych zagrożeń System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego). 7.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia System musi posiadać możliwość włączenia “automatycznej ochrony” w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykona w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail	

	bądź bramki sms, blokowanie hosta na którym występuje zagrożenie.	
MODUŁ RAPORTÓW	8.1. Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administrator musie mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.	
PANEL UŻYTKOWNIKA	9.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www. Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA. 9.2. Wizualizacja statystyk zdarzeń i logów Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod	

	kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości “nowych” zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania. 9.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo”. Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na “żywo”, a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę). 9.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd. Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów. 9.5. Intuicyjny panel zarządzania regułami i definiowania “customowych” logów. Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie	

	których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania “customowymi” logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych “customlogów” wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu “customlogów” musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.	

2. Serwer z macierzą dyskową SSD 1 szt.

Nazwa parametru lub wymaganej funkcjonalności	Charakterystyka (wymagania minimalne)	Opis oferowanej funkcjonalności lub parametru
1	*2*	*3*
Obudowa	Typu RACK, wysokość nie więcej niż 1U; Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable; Możliwość zainstalowania 8 dysków twardych hot plug 2,5"; Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; Zainstalowane 8 szt. dysków SSD SATA 960 GB Hot-Plug, dyski skonfigurowane w RAID-10 podłączone do sprzętowego kontrolera RAID; Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray	
Płyta główna	Dwuprocesorowa; Wyprodukowana i zaprojektowana przez producenta serwera; Możliwość instalacji procesorów 60-rdzeniowych; Moduł TPM 2.0; 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5; Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH; 32 gniazda pamięci RAM; Obsługa 8 TB pamięci operacyjnej RAM DDR4; Wsparcie dla technologii: Memory Scrubbing; SDDC; ECC; Memory Mirroring; ADDDC;	

	Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug. BIOS UEFI w specyfikacji 2.7.	
Procesory	Min 2 procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64;osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.	
Pamięć RAM	*Min 128 GB pamięci RAM;* *DDR5 Registered 4800MT/s;*	
Kontrolery LAN	Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: Min 5x 1G Base-T; Min 2x 10Gbit SFP+, porty obsadzone modułami SR LC; Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; Kontrolery I/O Kontroler SAS RAID dla dysków wewnętrznych obsługujący RAID 0,1,10 5;	
Porty	Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; Min 2 porty USB 3.0 dostępne z tyłu serwera; Min 2 porty USB 3.0 na panelu przednim; Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera	

Zasilanie, chłodzenie	Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; Redundantne wentylatory hotplug	
Zarządzanie	Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express; procesory CPU; pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; status karty zarządzającej serwera; wentylatory; bateria podtrzymująca ustawienia BIOS płyty głównej; zasilacze; system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym); Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; Dostęp poprzez przeglądarkę Web, SSH; Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; Zarządzanie alarmami (zdarzenia poprzez SNMP); Możliwość przejęcia konsoli tekstowej; Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); Obsługa serwerów proxy (autentykacja);	

	Obsługa VLAN; Możliwość konfiguracji parametru Max. Transmission Unit (MTU); Wsparcie dla protokołu SSDP; Obsługa protokołów TLS 1.2, SSL v3; Obsługa protokołu LDAP; Integracja z HP SIM; Synchronizacja czasu poprzez protokół NTP; Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. Wspierane OS Microsoft Windows Server 2022, 2019; VMWare vSphere 8.0;; Suse Linux Enterprise Server 15; Red Hat Enterprise Linux 9, 8; Microsoft Hyper-V Server 2019	
Gwarancja	Min 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.	

	Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu; Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).	
Dokumentacja, inne	Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego	

	serwerów. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV. Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04; Zgodność z normami: CB, RoHS, WEEE, GS oraz CE	
Oprogramowanie	1) Licencja na serwerowy system operacyjny Windows SVR 2025 lub oprogramowanie równoważne - system musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Licencja musi w pełni pokrywać licencyjnie rdzenie fizyczne zaproponowanego serwera oraz liczbę użytkowników w ilości min 30 szt. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 2) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 3) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.	

	4) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 5) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 7) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 8) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 9) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 10) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 11) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 12) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.	

	13) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 14) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 15) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 16) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 17) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 18) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 19) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 20) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 21) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 22) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 23) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.	

	24) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 25) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 26) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.	

	iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6),	

	k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez	

	oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 27) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 28) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 29) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 30) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 31) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim	

3. UPS typ 1 -1 szt.

Nazwa parametru lub wymaganej funkcjonalności	Charakterystyka (wymagania minimalne)	Opis oferowanej funkcjonalności lub parametru
1	*2*	*3*
Moc	Min moc 3000VA/3000W,	
Parametry wejściowe	• Napięcie: 230 V (1-fazowe), tolerancja 115 – 280 V • Częstotliwość: 50/60 Hz, tolerancja 40-70 Hz Współczynnik mocy/THDi : > 0,99 / < 5 %	
Parametry wyjściowe:	• Napięcie (czysty przebieg sinusoidalny): 230V • Częstotliwość: 50 Hz • Współczynnik mocy 1 • Sprawność: 94 % w trybie on-line • Przeciążalność: min. 105 % w sposób ciągły; 125 % przez 5 min; 150 % przez 60 s Liczba i rodzaj gniazdek z utrzymaniem zasilania 1 x IEC320 C19 (16A), min 6 x IEC320 C13 (10A	
Bateria	• Hermetyczne, bezobsługowe akumulatory typu VRLA AGM muszą zapewnić czas podtrzymania minimum 15 minut dla obciążenia 1200 W, minimum 4 min dla mocy 2700W • Bateria wbudowana w zasilacz UPS obsługa min 10 zewnętrznych modułów bateryjnych	
Zasilacz UPS musi być zgodny z Normami	• Parametry i topologia: IEC 62040-3 (VFI-SS-111) • Bezpieczeństwo: IEC/EN 62040-1 • Kompatybilność elektromagnetyczna IEC/EN 62040-2, kat. 2 • ESD: EN61000-4-2 poziom4, kryteria A • Podatność na wyemitowane zakłócenia: IEC/EN 61000-4-2	

	• Certyfikaty: CE Stopień ochrony: IP20	
Zasilacz UPS musi spełniać parametry środowiskowe, co najmniej takie jak:	• Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C) • Wilgotność: 0-95 % bez kondensacji Poziom hałasu w odległości 1 m od przodu urządzenia: < 55 dB	
Parametry	• Wymiary zasilacza UPS nie mogą być większe niż: szer. x głęb. x wys. (mm) 430 × 540 × 85 • Waga: 28,2 kg	
Komunikacja	Zasilacz UPS musi być wyposażony w kartę SNMP, wbudowany port EPO (konfigurowalny NO/NC) oraz gniazda USB, RS232 i RS485.	

4. Przełącznik 1 szt.

Nazwa parametru lub wymaganej funkcjonalności	Charakterystyka (wymagania minimalne)	Opis oferowanej funkcjonalności lub parametru
1	*2*	*3*
Warstwa przełączania	• L2 L3	
Architektura sieci	GigabitEthernet	
Liczba portów 10/100/1000 Mbps	Min 24	
Liczba portów 10Gb	Min 2	
Liczba portów SFP+	Min 2	
Przepustowość	Min 44 Gb/s	
Prędkość przekazywania	Min 65.472 Mpps	
Możliwość łączenia w stos	Min Tak	
Bezpieczeństwo	Ochrona ESD / EMP: Powietrze: 16 kV, Kontakt: 12 kV	
Typ obudowy	Rack	
Zasilacz	Wewnętrzny	

Pobór mocy	Max 30 W	
Zasilanie	AC / DC, 36 W.	
Wymiary	Max 442,4 x 285,4 x 43,7 mm	
Waga	Max 3,5 kg	
Informacje o gwarancji	Min Gwarancja 36 miesięcy	

5. UPS typ 2 - 5 szt.

Nazwa parametru lub wymaganej funkcjonalności	Charakterystyka (wymagania minimalne)	Opis oferowanej funkcjonalności lub parametru
1	*2*	*3*
Moc pozorna	Min 600 VA	
Moc czynna	Min 360 W	
Czas podtrzymania (obciążenie 100%)	Min 3 min	
Czas ładowania	Max 4h	
Typ obudowy	TOWER	
Zabezpieczenia / filtry	Nadmierne rozładowanie Przeciw przeciążeniowe	
Funkcje specjalne	- Zimny start - Układ automatycznej regulacji napięcia (AVR) - Sinus podczas pracy na baterii **Diody informujące o:** - Ładowaniu baterii - Przeciążeniu UPSa - Słabej baterii - Przeciążeniu - Koniecznej wymianie baterii - Awarii akumulatora	
Porty zasilania wy.	2 x typ C/F (Schuko)	

Wymagania środowiskowe	- Temperatura pracy: od 0 do 40 stopni C - Temperatura przechowywania: od -20 do 50 stopni C - Wilgotność otoczenia pracy/przechowywania: 0 - 90% (bez kondensacji)	
Pozostałe parametry	- Min moc rzeczywista: 360W - Min Złącze wejściowe: kabel z wtykiem Schuko (10A) - Min czas podtrzymania przy obciążeniu 50%: 6 minut	

6. Zakup usługi konfiguracyjnej pozwalającej wdrożyć nowe rozwiązania informatyczne.

Nazwa parametru lub wymaganej funkcjonalności	Charakterystyka (zakres usługi)	Potwierdzenie zaoferowania usługi
1	*2*	*3*
Usługa konfiguracyjna	Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack. Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać dostarczone w miejsce wskazane przez Zamawiającego, zamontowane, skonfigurowane i uruchomione. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń Podłączenie całości rozwiązania do infrastruktury Zamawiającego Wykonanie procedury aktualizacji firmware dostarczonych elementów środowiska teleinformatycznego do najnowszej stabilnej wersji oferowanej przez producenta sprzętu Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające, kable zasilające). Usluga konfiguracji: Oprogramowania SIEM Wykonawca/dostawca musi: posiadać kompetencje na usługi związane z projektowaniem i wdrażaniem systemów informatycznych poświadczone certyfikatem ISO 9001 oraz 27001.	***TAK/NIE****

	posiada potencjał osobowy, tj. w trakcie realizacji zamówienia dysponuje lub będzie dysponował osobami o odpowiednich kwalifikacjach zawodowych, posiadającą wiedzę i doświadczenie niezbędne do wykonania zamówienia, tj.: co najmniej jedną osobą posiadającą kwalifikacje do wdrożenia oferowanego systemu klasy SIEM (poświadczone certyfikatem producenta oferowanego systemu klasy SIEM, lub poświadczeniem równoważnym, np. referencją wystawioną na tą osobę z wdrożenia oferowanego systemu klasy SIEM) 1. Przygotowanie serwera pod system klasy SIEM 2. Instalacja systemów operacyjnych na maszynach wirtualnych 3. Instalacja oprogramowania na maszynach wirtualnych 4. Konfiguracja oprogramowania 5. Przygotowanie paczek pod automatyczną instalację agentów systemu SIEM na końcówkach Konfiguracja serwer usługa uruchomienia serwera: konfiguracja RAID, instalacja systemu operacyjnego, poprawek, VM w tym AD, - testy bezpieczeństwa odtwarzania systemu Recovery w przypadku awarii - konfiguracja kopii zapasowej konfiguracja oprogramowania System zasiania gwarantowanego UPS Instalacja UPS, podłączenie do systemu rozdzielne, uruchomienie, wykonanie testów obciążeniowych Uruchomienie, testy dostarczonego obciążeniowe zasilacza UPS, instalacja oprogramowania w celu wyłączania bezpiecznego urządzeń podpiętych do zasilacza UPS Przełączniki sieciowe min. Warstwy przełączeniowej 2 z potami 10 Gb Konfiguracja adresacji zgodniej z adresacją zamawiającego i sieci V-lan umożliwiających podłączenia dostarczanej infrastruktury i jej bezpieczne separowanie	

***Wybrać odpowiednie.**