Załącznik nr 1A do SIWZ
Załącznik nr 1 do Opisu Przedmiotu Zamówienia
AZAPUZA/33/20/PN

Specyfikacja przedmiotu zamówienia w obszarze infrastruktury teleinformatycznej.

1. Specyfikacja dostarczanej infrastruktury informatycznej i architektury technicznej.

PRZEDMIOT ZAMÓWIENIA ZOSTAŁ PODZIELONY NA 2 CZĘŚCI (2 PAKIETY)

PAKIET NR 1 – CZĘŚĆ 1 ZAMÓWIENIA:

Pakiet	Typ	Liczba zamawianego sprzętu (sztuk)
Pakiet 1	**Laptop z myszą, systemem operacyjnym oraz oprogramowaniem biurowym**	12
Pakiet 1	**Komputer stacjonarny z klawiaturą, myszą i monitorem oraz z systemem operacyjnym i oprogramowaniem biurowym .**	12

W poniższej tabeli przedstawiono typy oraz liczbę zamawianej infrastruktury teleinformatycznej.

Tabela 1. Typy oraz liczba zamawianej infrastruktury teleinformatycznej.

PAKIET NR 2 – CZĘŚĆ 2 ZAMÓWIENIA

Pakiet	Typ	Liczba zamawianego sprzętu (sztuk)
Pakiet 2	**System do zarządzania informacją i zdarzeniami bezpieczeństwa SIEM (Security Information and Event Management)** wraz z konfiguracją i instruktażem stanowiskowym użytkowników wskazanych przez Zamawiającego	**1**
Pakiet 2	**System DAM (Database Activity Monitoring)** wraz z konfiguracją i instruktażem stanowiskowym użytkowników wskazanych przez Zamawiającego	**1**

W poniższej tabeli przedstawiono szczegóły dotyczące planowanej do zamówienia infrastruktury teleinformatycznej.

SZCZEGÓŁOWY OPIS PARAMETRÓW TECHNICZNYCH – 1 CZĘŚĆ ZAMÓWIENIA – PAKIET NR 1 ZAMÓWIENIE PODSTAWOWE

Tabela 2. Szczegóły zamawianej infrastruktury teleinformatycznej w podziale na komponenty.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
Laptop z myszą, systemem operacyjnym oraz oprogramowaniem biurowym - dostawa		
1.	Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
2.	Przekątna ekranu	15,6” FHD (1920 x 1080), z powłoką przeciwodblaskową, jasność 220 nits
3.	Procesor	Wynik procesor osiąga w teście PassMark Performance Test co najmniej 6940 punktów w Passmark CPU Mark. Dostępny na stronie: http://www.passmark.com/products/pt.htm
4.	Pamięć RAM	16GB DDR4 2400MHz możliwość rozbudowy do min 32GB, 2 sloty na pamięci w tym min. jeden wolny
5.	Pamięć masowa	256GB NVMe SSD M.2
6.	Karta graficzna	Zintegrowana karta graficzna osiągająca w teście PassMark Performance Test co najmniej 880 punktów w G3D Rating. Dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
7.	Klawiatura i mysz	Klawiatura z wbudowanym w klawiaturze podświetleniem, (układ US), min 100 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Nie dopuszcza się innego układu a w szczególności między klawiszami ALT i CTRL (oprócz klawisza FN i Windows z lewej strony) Mysz optyczna, czarna.
8.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy. czytnik kart microSD, 1 port audio typu combo (słuchawki i mikrofon)
9.	Łączność bezprzewodowa	Intel® Wi-Fi 6 AX201 2x2 + Bluetooth 5.1
10.	Bateria i zasilanie	Bateria Polymer nin. 4-cell [min. 53Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 65W
11.	Waga i wymiary	Waga max 2kg z baterią 4-cell Suma wymiarów notebooka nie większa niż 640mm
12.	Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Komputer spełniający normy MIL-STD-810G [załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta]
13.	BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag. Możliwość ustawienia hasła dla administratora, możliwość ustawienia hasła dla użytkownika które jednocześnie będzie blokować uruchamianie systemu z jakichkolwiek urządzeń, możliwość konfiguracji zależności między tymi hasłami, hasła muszą umożliwiać zawarcia w sobie znaków specjalnych, liczb i liter, Możliwość odczytania informacji o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
14.	Certyfikaty	Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty) Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) EnergyStar – załączyć do oferty certyfikat lub wydruk z strony. Certyfikat TCO, wymagana certyfikacja na stronie: https://tcocertified.com/product-finder/ – załączyć do oferty wydruk z strony.
15	Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
16.	Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czytnik linii papilarnych
17.	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiający instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, lub równoważny*.
18.	Oprogramowanie dodatkowe	Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji : a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
19.	Oprogramowanie biurowe	Microsoft Office Home & Business 2019 PL lub równoważne*
20.	Porty i złącza	Wbudowane porty i złącza: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.1, 1x USB TYP-C z obsługą DP 1.2, 1x USB 2.0, port zasilania, złącze linki zabezpieczającą
21.	Warunki gwarancyjne, wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) 3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta
Komputer stacjonarny z klawiaturą, myszą i monitorem oraz z systemem operacyjnym i oprogramowaniem biurowym - dostawa		
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
3.	Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 6940 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
4.	Pamięć RAM	16GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. Jeden slot DIMM wolny.
5.	Pamięć masowa	Dysk M.2 SSD 256GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”.
6.	Wydajność grafiki	Zintegrowana karta graficzna osiągajaca w teście Passmark G3D Mark, w kategorii Average G3D Mark wynik co najmniej 880 pkt. według wyników opublikowanych na stronie https://www.videocardbenchmark.net/gpu_list.php
7.	Wyposażenie multimedialne	Karta dźwiękowa min. czterokanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
8.	Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		Procedura POST traktowana jest jako oddzielna funkcjonalność.
9.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		poszczególnych komponentów systemu).
11.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
12.	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub równoważny*.
13.	Oprogramowanie biurowe	Microsoft Office Home & Business 2019 PL lub równoważny*
14.	Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE (załączyć do oferty) Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
15.	Wymagania dodatkowe	Wbudowane porty: • 1 x HDMI 1.4 • 1 x DisplayPort 1.4 • 1 x VGA • 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: o Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 o Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 • 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu • 1 x port audio-out na tylnym panelu obudowy • 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie US/International Mysz USB z dwoma klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
16.	Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
17.	Warunki gwarancji	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego przedłużenia tego okresu do 4 lub 5 lat od daty dostawy. Sposób realizacji usług wsparcia technicznego: • Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. • Dedykowany bezpłatny portal online producenta do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. • Opcjonalna pomoc techniczna za pośrednictwem czat online. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. Zamawiający wymaga od podmiotu realizującego serwis lub producenta

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
18.	Dodatkowe oprogramowanie	Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego. Oprogramowanie musi w pełni integrować się z Microsoft SCCM Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego.
Monitor		
1.	Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 23,8”
2.	Rozmiar plamki (maksymalnie)	0,275 mm x 0,275 mm
3.	Jasność	250 cd/m2
4.	Kontrast	1000:1
5.	Kąty widzenia (pion/poziom)	178/178 stopni
6.	Czas reakcji matrycy (maksymalnie)	5ms (gray to gray) w trybie fast 8ms (gray to gray) w trybie normal
7.	Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
8.	Gama koloru	min. 82% (CIE 1976) min. 72% (CIE 1931)
9.	Częstotliwość odświeżania poziomego	30 – 83 kHz
10.	Częstotliwość odświeżania pionowego	56 – 76 Hz
11.	Pochylenie monitora	W zakresie 26 stopni
12.	Wydłużenie w pionie	Tak, min 130 mm
13.	PIVOT	Tak
14.	Obrót lewo/prawo	Min. 90 stopni
15.	Powłoka powierzchni ekranu	Antyodblaskowa
16.	Podświetlenie	System podświetlenia LED
17.	Zużycie energii	Typowo 18W, maksymalne 42W, czuwanie mniej niż 0,3W Energy Star nie więcej niż 17W
18.	Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
19.	Waga bez podstawy	Maksymalnie 3,27kg
20.	Waga z podstawą	Maksymalnie 5,26kg
21.	Złącze	1x 15-stykowe złącze D-Sub, 1x HDMI (v1.4), 1x złącze DisplayPort (v1.2) 2 x USB 3.0 (na bocznej ściance monitora) 1 USB 3.0 port - upstream 2 x USB 2.0 ports (w tylnej obudowie monitora)
22.	Gwarancja	3 lata na miejscu u klienta

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
		Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Gwarancja zero martwych pikseli
23.	Certyfikaty	ISO 13406-2 lub ISO 9241, EPEAT Gold, Energy Star Monitor musi się znajdować na stronie TCO : http://tcocertified.com/product-finder/
24.	Inne	Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej. Odłączany stand bez użycia narzędzi VESA 100mm. Możliwość podłączenia do obudowy dedykowanych głośników

* **Warunki równoważności na dostarczane oprogramowanie**

Zamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia, jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilne w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia. W przypadku zaproponowania wersji równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego.

Za rozwiązanie równoważne Zamawiający uznaje rozwiązanie, które nie spowoduje poniesienia dodatkowych kosztów (np. dodatkowych licencji, dodatkowego sprzętu, kosztów związanych z modyfikacją systemów działających u Zamawiającego, itp.) po stronie Zamawiającego.

SZCZEGÓŁOWY OPIS PARAMETRÓW TECHNICZNYCH – 2 CZĘŚĆ ZAMÓWIENIA (PAKIET NR 2)

System do zarządzania informacją i zdarzeniami bezpieczeństwa SIEM (Security Information and Event Management)		
1.	Funkcjonalności	1. System do zarządzania informacją i zdarzeniami bezpieczeństwa. (SIEM Security Information and Event Management). Jego zadaniem jest obsługa i wykrywanie zagrożeń oraz reagowanie na incydenty związane z zagrożeniem bezpieczeństwa w zakresie sieci komputerowej oraz systemów serwerowych. System w formie maszyny wirtualnej uruchomionej w infrastrukturze Zamawiającego lub dostarczenie dedykowanego urządzenia. 2. System musi zapewniać minimum 1000 EPS, minimum 100 urządzeń jako źródeł zdarzeń, w tym minimum 50 komputerów Windows z wykorzystaniem dostarczonego w ramach systemu oprogramowania typu agent; 3. 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 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 mają one mieć możliwość buforowania otrzymanych informacji d. Kolektory muszą mieć możliwość kompresowania danych przesyłanych do warstwy przechowującej i korelującej e. Kolektory muszą mieć możliwość ograniczania przepustowości z którą zdarzenia są przesyłane do warstwy przechowującej i korelującej f. Komunikacja pomiędzy warstwą przechowującą i korelującą musi odbywać się z wykorzystaniem protokołu HTTPS. Odbywa się ona w kierunku od kolektorów do warstwy przechowującej i korelującej g. 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 h. Wydajność kolektora nie może być mniejsza niż 5 000 EPS i. Kolektory muszą być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu NetFlow j. Poszczególne kolektory muszą być w stanie automatycznie aktualizować nowe parsery wtedy gdy zostaną one zaktualizowane w centralnym systemie zarządzającym rozwiązaniem SIEM k. Kolektory mają mieć możliwość aktualizacji z warstwy przechowującej i korelującej 4. Warstwa przechowywania i korelacji danych, od tego miejsca okre-

		ślana jako Klaster SIEM, ma spełniać następujące wymagania: a. implementacja ma być zrealizowana w oparciu o maszyny wirtualne (VA - Virtual Appliance) b. 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 c. rozwiązanie ma wspierać nie mniej niż poniżej wymienione środowiska wirtualizacyjne: • VMWare • Hyper-V • KVM • AWS • Azure d. Klaster SIEM może skalować się poprzez dodawanie kolejnych maszyn wirtualnych (Virtual Appliance - VA). Wspomniana skalowalność ma być realizowana również poprzez: • przeprowadzaną w czasie rzeczywistym, w pamięci rozwiązania, dystrybuowaną pomiędzy elementy klastra korelację reguł • dystrybuowanie pomiędzy elementy 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 gromadzonych i przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie może być rozmiar przestrzeni dyskowej f. Skalowalność rozwiązania SIEM ma również wynikać z możliwości dodawania kolejnych maszyn wirtualnych. Dane zbieranych zdarzeń (events) mogą być gromadzone na dyskach maszyn wirtualnych 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). g. Klaster SIEM musi mieć możliwość obsłużenia (potencjalną możliwość docelowego wyskalowania do) nie mniej niż 500 tys. EPS. h. 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 i. 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 j. Zebrane dane muszą być przechowywane w sposób skompresowany k. System musi mieć możliwość anonimizacji zebranych danych w

		zakresie nie mniejszym niż: adresy IP, nazwy hostów, adres MAC, 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. l. Klaster SIEM nie może wykorzystywać 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 dawać możliwość integracji z Elasticsearch m. Relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania, szablonów, zdarzeń i innych ustrukturyzowanych informacji n. Maszyny wirtualne systemu SIEM mają działać w oparciu o system Linux który ma mieć możliwość aktualizacji 5. 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 jak: • SNMP • WMI • VM SDK • OPSEC • JDBC • Telnet • SSH • JMX • import z pliku CSV • import z pliku PCAP b. zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP/SCP, TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, 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): • wersja oprogramowania/firmware/systemu operacyjnego • numer seryjny urządzenia • skonfigurowane interfejsy wraz z: ▪ nazwą interfejsu ▪ adresem IP oraz podsiecią

		▪ statusem interfejsu (włączony, wyłączony) ▪ informacją o skonfigurowanych poziomach bezpieczeństwa ▪ prędkością interfejsu ▪ możliwością edycji nazwy oraz prędkości interfejsu • procesach działających na urządzeniu lub systemie operacyjnym • alarmach w przypadku zmiany statusu procesu np. jego uruchomienia lub zatrzymania (monitoring w oparciu protokoły opisane w 3a) d. możliwość automatycznego przypisania do grupy poszczególnych 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 f. raportowanie informacji zawartych w bazie urządzeń (CMDB), w tym takich jak: i. raportowanie na temat firmware'u poszczególnych urządzeń lub numeru jego wersji ii. raport audytowy z informacją typu "pass/fail" analizujący czy określone urządzenia działają z właściwą wersją firmware'u/systemu operacyjnego g. 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. Metody pobierania danych zostały określone w punkcie 3.a h. zbieranie metryk wydajnościowych ma dotyczyć nie mniej niż: • utylizacji interfejsów sieciowych, występujących tam błędów, ilości wysłanych i odebranych danych (np. bajtów) • obciążenia CPU • wykorzystania pamięci • wykorzystania przestrzeni dyskowej • utylizacji poszczególnych procesów 6. 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 7. 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 8. Zarówno dane w stanie surowym jak i ten sparsowane lub wzbogacone muszą być możliwe do przesłania do rozwiązania SIEM z kolektorów

		9. Przetwarzanie danych związanych z poszczególnymi zdarzeniami (events) wykonywane jest poprzez parsery systemowe 10. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów 11. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI) 12. 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) 13. 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 14. Musi istnieć możliwość monitorowania urządzeń bez wykorzystania aplikacji typu agent oraz poprzez SSH, telnet, WMI, JMX oraz PowerShell 15. Rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu aplikacje typu agent 16. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości: a. centralne zarządzanie 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 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 17. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości: a. centralne zarządzanie 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 proces ro-

		dzimy oraz sumę kontrolną 18. System SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administation) celem ograniczania dostępu do danych oraz do GUI 19. System SIEM musi być w stanie wykryć usługi Active Directory oraz LDAP oraz wyświetlać informacje o strukturze katalogowej drzewa w GUI 20. Musi istnieć możliwość wykorzystania struktury katalogowej drzewa jako warunku podczas tworzenia raportów i w ramach pozostałych mechanizmów analitycznych 21. Muszą być wspierane zewnętrzne metody uwierzytelniania, nie mniej niż: a. Active Directory b. LDAP c. RADIUS 22. Musi istnieć integracji 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: • adresy IP • domeny • sumy kontrolne (hash) • adresy URL c. wymagane jest aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 200 tyś wpisów d. wraz z systemem SIEM musi być dostarczony, już zintegrowany, zestaw komercyjnych baz zagrożeń e. wraz z systemem SIEM musi być dostarczony, 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. rozwiązanie musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK 23. 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 24. 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 h. GPG13 i. SANS Critical Controls 25. System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML 26. System SIEM musi pozwalać na zbieranie konfiguracji urządzeń, identyfikowanie zmian w nich następujących wraz z możliwością porównywania poszczególnych wersji obok siebie 27. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji 28. 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 trzech kolorach mogą być definiowane na poszczególnych wykresach 29. Notyfikacje oraz zarządzanie incydentami System SIEM musi: a. posiadać narzędzia pozwalające na samodzielne tworzenie polityk informujących o incydentach b. posiadać możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty c. posiadać możliwość integracji w oparciu o API z zewnętrznymi systemami do obsługi zgłoszeń (ticketing systems) takimi jak ServiceNow, ConnectWise oraz Remedy d. mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) e. mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) 30. 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 typu SQL, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regu-

		larne, wyrażenia matematyczne. Opisane możliwości mają być dostępne zarówno na GUI jak i API e. wyszukiwania w oparciu o nie mniej niż następujące operatory: include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex f. podejmowania w czasie rzeczywistym działań w oparciu o złożone wzorce zdarzeń • w przypadku prostych zapytań musi na przykład być możliwe określenie wartości granicznej (threshold) ilości zdarzeń X w określonym przedziale czasowym Y z Z wybranych wartości • 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 a. analiza statystyczna i alarmowanie w oparciu o zdarzenia musi mieć możliwość działania w oparciu o: i. średnie kroczące (moving averages) ii. odchylenia standardowe (standard deviations) b. w wypadku przekroczenia statystycznej wartości granicznej (statistical threshold) musi zostać wygenerowany alert w czasie zbliżonym do rzeczywistego g. wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenie reguł h. tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną wraz z możliwością eksportowania do formatów CSV i PDF i. wyszukiwania zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego j. wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej k. skalowania możliwości analitycznych poprzez dodawanie do systemu SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego klastra SIEM l. automatycznego korelowania użytkownika z jego lokalizacją i adresem IP: • musi istnieć możliwość tworzenia raportów i wyszukiwania użytkownika w połączeniu z jego adresem IP oraz lokalizacją. Lokalizacja może oznaczać port na przełączniku, adres MAC lub połączenie VPN • musi istnieć możliwość wzbogacania zdarzeń (events) przy

		których dane użytkownika pozbawione są informacje o adresie IP • wykorzystanie funkcjonalności Geo IP w oparciu o bazę pochodzącą od tego samego producenta m. możliwość wykrywania zdarzeń IPS false positive w oparciu o integrację z zewnętrznymi skanerami podatności 31. System SIEM musi pozwalać na przesłanie dowolnych zebranych zdarzeń z wykorzystaniem protokołu KAFKA 32. System SIEM musi pozwalać na realizowane w oparciu o polityki archiwizowanie danych do innego udziału, takiego jak np. NFS. Musi istnieć możliwość odtwarzania tych danych z wykorzystaniem GUI 33. Integralność danych 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 34. Użyteczność oraz dojrzałość technologiczna zaoferowanego rozwiązania musi być potwierdzona obecnością producenta rozwiązania w Magicznym Kwadrancie Gartnera (MQ) dla Security Information and Event Management (SIEM) z 2020 roku. 35. Dodatkowe wymagania: W ramach realizacji przedmiotu zamówienia, Wykonawca będzie zobowiązany do: - wdrożenia i konfiguracji systemu oraz - przeprowadzenia instruktaży stanowiskowych użytkowników wskazanych przez Zamawiającego
System DAM (Database Activity Monitoring)		
1.	Funkcjonalności:	Celem systemu ma być ochrona dostępu do danych przetwarzanych w bazach danych poprzez monitorowanie w czasie rzeczywistym wszelkich aktywności realizowanych na poziomie baz danych oraz przeciwdziałanie potencjalnym zagrożeniom, Ilość zabezpieczanych baz danych Min. 5 Wspierane technologie MS SQL Server, Oracle, MySQL, PostgreSQL Technologia: System DAM w postaci urządzenia lub VM dla Vmware 6.7 lub wyższy Dodatkowe wymagania: W ramach realizacji przedmiotu zamówienia, Wykonawca będzie zobowiązany do: - wdrożenia i konfiguracji systemu oraz - przeprowadzenia instruktaży stanowiskowych użytkowników wskazanych przez Zamawiającego

*** Warunki równoważności na dostarczane oprogramowanie**

Zamawiający uzna, że zaoferowane rozwiązanie posiada równoważne cechy z przedmiotem zamówienia, jeżeli będzie ono zawierało funkcjonalności co najmniej tożsame lub lepsze od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilne w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia. W przypadku zaproponowania wersji

równoważnej Wykonawca zobowiązany jest załączyć do oferty opis i dane techniczne zaproponowanego rozwiązania umożliwiające porównanie go z wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym zgodność posiadanego oprogramowania z zaproponowanym rozwiązaniem. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia wykonawca jest zobowiązany w terminie 5 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego.
Za rozwiązanie równoważne Zamawiający uznaje rozwiązanie, które nie spowoduje poniesienia dodatkowych kosztów (np. dodatkowych licencji, dodatkowego sprzętu, kosztów związanych z modyfikacją systemów działających u Zamawiającego, itp.) po stronie Zamawiającego.