IB.271.4.2024

Opis przedmiotu zamówienia dla zadania:

Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM,SOAR wraz z serwerem tworzącym platformę sprzętową dla SOC oraz oprogramowaniem do monitorowania sieci w ramach zadania „Cyberbezpieczny samorząd".

Zakres przedmiotu zamówienia:

1. Dostawa i kompleksowe wdrożenie serwera tworzącego platformę sprzętową dla SOC
2. Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM,SOAR (Security Information and Event Management, Security Orchestration, Automation and Response)
3. Dostawa i wdrożenie oprogramowania do monitorowania i zarządzania siecią

Wymagania dla pkt 1

Dostawa i kompleksowe wdrożenie serwera tworzącego platformę sprzętową dla SOC	
1.	Pamięć RAM o pojemności minimum 96GB w kościach DDR4, o taktowaniu minimum 3200MHz, kości pamięci wyposażone w system kodowania korekcyjnego ECC, możliwość rozszerzenia pamięci RAM maksymalnie do 12 TB (6TB na procesor).
2.	Zainstalowane dwa procesory 16 rdzeniowe/32 wątkowe o taktowaniu minimalnym 2.4GHz i TDP max 135W, każdy procesor powinien osiągać wynik minimum 29 tys. pkt benchmark w teście cpubenchmark.net.
3.	Zainstalowane dedykowane do danego serwera chłodzenie procesorów umożliwiające poprawną pracę systemu.
4.	Powinien posiadać mechanizm hot-swap i obsługiwać do 12 dysków.
5.	Zainstalowany dedykowany kontroler RAID, posiadający możliwość obsługi co najmniej 4 dysków w tym SATA/SAS, kontroler musi wspierać minimum RAID 0,1,10.
6.	Zainstalowane co najmniej dwa dyski SSD klasy enterprise, o pojemności nie mniejszej niż 480GB każdy, dyski przeznaczone na system operacyjny powinny pracować w RAID 1.
7.	Zainstalowane co najmniej dwa dyski HDD klasy enterprise, o pojemności nie mniejszej niż 4TB każdy.
8.	Karta sieciowa 10Gb posiadająca minimum 2 porty RJ45.
9.	Do zestawu dołączony napęd DVD, dopuszczony jest także napęd zewnętrzny.
10.	Serwer powinien posiadać zasilanie redundantne z dwoma zasilaczami klasy minimum Platinium o mocy minimum 1300W każdy, dedykowane do danego modelu serwera, zasilacze powinny posiadać mechanizm hot-swap, do zasilaczy dołączone 2 przewody zasilające.
11.	Zainstalowany system operacyjny (przeznaczony dla serwera) opublikowany najpóźniej w 2021 r. posiadający licencje na obsługę wszystkich rdzeni zamontowanych procesorów.

12.	Serwer powinien być wyposażony w moduł TPM 2.0 lub równoważny.
13.	Płyta główna dedykowana do serwera posiadająca obsługę minimum 2 procesorów, płyta musi mieć możliwość rozszerzenia funkcjonalności serwera o kolejne karty rozszerzeń pod złącza PCI-e.
14.	Zintegrowana karta graficzna ze złączem VGA lub pokrewnym,
15.	Serwer powinien mieć możliwość optymalizacji pod kątem wirtualizacji.
16.	Sprzęt wyprodukowany zgodnie z normami ISO 9001 lub równoważna, ISO 14001 lub równoważna oraz CE lub równoważna,
17.	Możliwość weryfikacji na stronie producenta specyfikacji serwera, okresu gwarancji oraz pobrania najnowszych sterowników po podaniu numeru seryjnego sprzętu.
18.	Zintegrowana karta zdalnego zarządzania posiadająca dedykowany port RJ45.
19.	Serwer powinien posiadać umożliwiać montaż w szafie RACK, wysokość serwera max 2U, do serwera dołączone szyny montażowe w zestawie.
20.	Gwarancja na okres minimum 24 miesiące, świadczona na miejscu u klienta (on-site) z czasem reakcji 24h (w dni robocze).
21.	Możliwość rozszerzenia gwarancji do minimum 5 lat w trakcie jej trwania
22.	Serwis realizowany przez producenta lub autoryzowanego partnera.
23.	Wykonawca przygotuje serwer pod platformę SOC w siedzibie zamawiającego. Poprzez przygotowuję uznaję się: zainstalowanie systemu operacyjnego oraz przeprowadzenie niezbędnej konfiguracji umożliwiającej prace.

Warunki gwarancji i serwisu oferowanych urządzeń		
1.	Okres gwarancji dostarczonego serwera	**Min 24 miesiące**
Dodatkowe wymagania		
Przedmiot zamówienia fabrycznie nowy, wolny od wad, może być użytkowany zgodnie z przeznaczeniem opisanym w instrukcji obsługi		
Gwarantowany czas przystąpienia do naprawy – maksymalnie 2 dni robocze od dnia zgłoszenia wady		
Gwarantowany czas naprawy wyposażeni – maksymalnie 14 dni roboczych od dnia zgłoszenia wady		
Wymiana wyposażenia na nowe, w przypadku, gdy ta sama wada będzie naprawiana więcej niż 3 razy		
Dostarczenie wyposażenia zastępczego, o parametrach nie gorszych niż będące przedmiotem naprawy, jeżeli czas naprawy wadliwego urządzenia będzie dłuższy niż 7 dni roboczych od dnia zgłoszenia wady		
Wymiana urządzenia lub jego części na wolne od wad, w przypadku wystąpienia wad niemożliwych do usunięcia – w terminie maksymalnie 14 dni roboczych od dnia zgłoszenia wady		

Wykonawca zobowiązuje się dostarczyć wraz z urządzeniami sporządzone w języku polskim dokumenty, wymienione w § 4 ust. 3 wzoru umowy.
Wykonawca potwierdza, że na własny koszt i we własnym zakresie dostarczy i zmontuje wyposażenie w miejscach wskazanych przez Zamawiającego.
Wykonawca wykona wszelkie niezbędne czynności w zakresie instalacji konfiguracji i uruchomienia dostarczonego sprzętu.

Wymagania dla pkt 2

Dostawa i kompleksowe wdrożenie systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM,SOAR (Security Information and Event Management, Security Orchestration, Automation and Response)	
Lp.	**Parametry wyposażenia**
1.	Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu do wykrywania i zarządzania incydentami, podatnościami i ryzykiem SIEM,SOAR z wszystkimi koniecznymi licencjami, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.
2.	System powinien zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji
3.	System powinien zawierać bazę wiedzy eksperckiej (tzw. Knowledge Base) uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.
4.	Dostarczone rozwiązanie powinno być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.
5.	Dostarczone rozwiązanie powinno być systemem klasy SOAR (Security Orchestration, Automation And Response). Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania.
6.	Interfejs systemu elektronicznej dokumentacji powinien umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej. Wizualizacja powinna obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.
7.	System powinien umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.

8.	System powinien prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je usługi i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów oraz zespół IT odpowiedzialny za jego obsługę.
9.	System powinien umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny (minimum: na podstawie danych pozyskanych z logów oraz poprzez API) lub za pomocą interfejsu graficznego i tabelarycznego.
10.	Interfejs interaktywnej mapy sieci powinien umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.
11.	System powinien pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.
12.	System powinien pozwalać na dodawanie i przechowywanie załączników powiązanych z obiektami zgromadzonymi w bazie elektronicznej dokumentacji sieci. System powinien akceptować załączniki między innymi w formatach: pdf, MS Word, MS Excel, JPG, PNG.
13.	Dla zdarzeń zawierających adresy IP interfejs powinien umożliwiać wyświetlenie dodatkowych informacji o zasobach powiązanych z tymi adresami m.in.: nazwa zasobu, rodzaj zasobu, powiązane usługi, właściciel zasobu, podatności zasobu, powiązane incydenty, lokalizacja.
14.	System powinien zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
15.	Dla zarejestrowanych zdarzeń/ incydentów system automatycznie wyznaczy ścieżkę ataku i zaprezentuje ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.
16.	Informacje o procesach muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).
17.	Mechanizmy modułu dokumentacji elektronicznej muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.
18.	System powinien pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np.: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).
19.	W ramach obsługi zdarzeń/incydentów/podatności system powinien prezentować informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem oraz ocenę wpływu incydentu na organizację w przypadku materializacji zagrożenia.

20.	System powinien pozwalać na zautomatyzowane szacowanie ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka powinno odbywać się względem zagrożeń natury informatycznej, np.: przełamanie zabezpieczeń, wyciek danych, infekcja złośliwym programem, podsłuch sieciowy.
21.	System w razie wykrycia incydentów o wysokim ryzyku materializacji zagrożenia natury technicznej (m.in. przełamanie zabezpieczeń, infekcja złośliwym oprogramowaniem) umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
22.	System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email i SMS.
23.	System powinien umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie krytycznych usług w organizacji.
24.	System ma posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa. Interfejs mapy sieci powinien pozwalać m.in. na: a. wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny, b. wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia, c. wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia, d. wyświetlanie lokalizacji zasobów określonego rodzaju, e. wyświetlanie najbardziej narażonych zasobów teleinformatycznych, f. wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.
25.	System powinien umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych)
26.	Rozwiązanie powinno umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE

27.	Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry: a. strefę bezpieczeństwa w której została wykryta podatność, b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, c. rodzaj zasobu którego dotyczy ta podatność, d. ważność tego zasobu dla organizacji, e. przetwarzane na tym zasobie informacje, np.: dane osobowe, f. usługi realizowane przez ten zasób, np.: DNS, g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact" = High, h. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.
28.	W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
29.	System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie.
30.	System powinien pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
31.	System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
32.	System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI.
33.	System powinien umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.
34.	System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
35.	System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

36.	Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
37.	System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.
38.	Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.
39.	System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
40.	System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
41.	System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
42.	System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
43.	System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
44.	Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.
45.	System powinien umożliwiać automatyczne dodawanie i usuwanie list referencyjnych na podstawie reguł korelacyjnych umożliwiających zdefiniowanie warunków na podstawie których listy te będą modyfikowane. System powinien umożliwiać definiowanie list referencyjnych łączących unikalne wartości w pojedynczym wierszu np.: login, adres IP, aplikacja, hash, nazwa procesu.

46.	System powinien być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych, system powinien tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.
47.	System powinien umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w scenariuszach obsługi incydentów. Scenariusze obsługi incydentów muszą być uzależnione od ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
48.	System powinien umożliwiać wykorzystanie baz reputacyjnych w ramach scenariuszy obsługi incydentów (ang. Playbook).
49.	System powinien zapewnić graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi: a. wzbogacanie danych kontekstowych, b. gromadzenie artefaktów danych związanych z incydentem, c. współpraca z innymi członkami zespołu, d. komunikacja w ramach zespołu, e. wykonywanie czynności związanych z reakcją na incydent, f. raportowanie przebiegu incydentu.
50.	System powinien być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów/podatności. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: ilość incydentów w czasie w podziale na priorytety, czasy reakcji i obsługi oraz bieżące ilości incydentów obsługiwanych przez poszczególnych użytkowników.
51.	System powinien posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook).
52.	Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.
53.	System powinien pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
54.	System powinien pozwalać na przekazywanie aktywnych linków pomiędzy zintegrowanymi systemami, a otwarcie linku powinno bezpośrednio przekierowywać operatora do konsoli systemu zewnętrznego.
55.	System powinien umożliwiać automatyczną zmianę statusu incydentu na podstawie informacji pobranych z innych systemów np.: identyfikacja IoC.

56.	System powinien umożliwiać zbieranie, przechowywanie i przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników: a) fqdn, b) e-mail, c) nazwa pliku, d) ścieżka do pliku, e) hash, f) adres IP, g) klucz rejestru, h) cmd.
57.	System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/).
58.	Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs", „Malicious domain" czy „Tor Exit Nodes").
59.	System powinien udostępniać automatyczny raport z wszystkich podjętych działań w ramach incydentu.
60.	System powinien być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych. Mechanizm powinien umożliwiać m.in. parsowanie warunkowe, parsowanie hierarchiczne, wzbogacanie zdarzeń o dodatkowe pola, mapowanie wartości, czy wykorzystanie gotowych parserów przy tworzeniu nowych.
61.	System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
62.	Parsowanie warunkowe i hierarchiczne powinno być konfigurowalne i obsługiwać następujące metody normalizacji: REGEX, JSON, XML, CEF, LEEF, SYSLOG. Musi umożliwiać wykorzystanie gotowych parserów jako elementów podrzędnych hierarchii oraz wykorzystywanie ich.
63.	Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.
64.	System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
65.	Proces normalizacji powinien wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
66.	System powinien umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.

67.	System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
68.	System powinien zapewnić normalizację (parsowanie) logów protokołami Syslog, TLS Syslog, Netflow, obsługiwać pliki płaskie (ang. flat file), zapytania do bazy danych poprzez sterownik ODBC oraz odbierać wiadomości email.
69.	Oferowane rozwiązanie powinno zapewniać możliwość zbierania logów z systemów Microsoft Windows poprzez mechanizm Windows Event Forwarding (WEF) bez konieczności instalowania dedykowanego oprogramowania w tych systemach.
70.	Normalizacja logów powinna posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
71.	Normalizacja powinna uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól, np. logowanie, wylogowanie, zmiana uprawnień, malware.
72.	System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
73.	System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
74.	Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).
75.	System w swoim działaniu powinien korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
76.	System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: a) rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, b) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, c) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, d) rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
77.	System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

78.	Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.
79.	Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić: a) wykrycie dowolnej treści w logach, b) wykrycie zmiany jednego z kilku pól, c) wykrycie zaniku wiadomości, d) wykrycie nowej wartości pola w zadanym okresie czasu, e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu, m) wykrycie skanowania portów.
80.	Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: a) wykrycie wystąpienia wartości pola na wybranej liście, b) wykrycie niewystępowania wartości pola na wybranej liście, c) wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony), d) wykrycie niewystąpienia pary wartości na wybranej liście (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).
81.	Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, c) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.
82.	Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

83.	Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji; b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;
84.	Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, c) wykrycie nieautoryzowanej usługi na serwerze, d) wykrycie nieautoryzowanego połączenia do usługi na serwerze, e) wykrycie nieautoryzowanego połączenia z serwera usług, f) wykrycie nieautoryzowanego połączenia do sieci Internet.
85.	Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
86.	Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
87.	Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, c) wykrycie zdarzeń o wysokim „severity" na zasobach posiadającego krytyczne podatności, d) wykrycie zdarzeń o wysokim „severity" do zasobów posiadających krytyczne podatności.
88.	Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na: a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny

89.	Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić: a) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, b) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, c) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.
90.	Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.: a) wykrycie anomalii na koncie uprzywilejowanym użytkownika, b) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, c) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, d) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, e) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
91.	System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać: a) sparsowane pola oraz ich wartości, b) atrybuty użytkowników z Active Directory, c) atrybuty komputerów z Active Directory, d) informacje z elektronicznej dokumentacji.
92.	Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: a) adresie IP, b) koncie domenowym użytkownika, c) strefie bezpieczeństwa, d) zakresie adresów IP.
93.	System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

94.	Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.
95.	Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
96.	W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.
97.	System powinien umożliwiać definiowanie zakresu i czasu uczenia, np.: analiza logowania użytkowników po godzinach pracy, analiza alarmów systemu SIEM. Po wdrożeniu nie będzie wymagane żadne dostrojenie systemu.
98.	System powinien mieć możliwość wzbogacania kontekstu odbiegającego od normalnego zachowania użytkownika korzystając z danych zewnętrznych, minimum: Threat Intelligence, Active Directory. Przykładowe zastosowanie integracji zakłada wykorzystanie zasobów zewnętrznych, z których dane mogą podnieść skumulowaną ocenę ryzyka dla sesji użytkownika.
99.	System powinien posiadać funkcję „automatycznej korelacji”, tzn. posiadać zaszyte mechanizmy i reguły korelacji, które po wdrożeniu i „nauce środowiska zamawiającego”, będą przedstawiać właściwe incydenty dla operatorów bez dodatkowej ingerencji w reguły.
100.	System powinien zapewniać możliwość budowania modeli zachowania użytkowników dla zebranych danych historycznych ze skonfigurowanego (wskazanego) okresu.
101.	Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych: a) kolektor parsujący; b) kolektor logów; c) kolektor korelacyjny; d) kolektor zdarzeń; e) kolektor sztucznej inteligencji; f) kolektor reakcyjny; g) kolektor kontrolujący.
102.	Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103.	Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.
104.	Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.
105.	Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).
106.	Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.
107.	Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.
108.	Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.
109.	Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.
110.	Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.
111.	Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.
112.	Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

113.	Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.
114.	System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.
115.	Rozwiązanie 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).
116.	System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi
117.	System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal.
118.	System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.
119.	Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.
120.	Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.
121.	System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 5 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.
122.	W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć.
123.	Dostarczone rozwiązanie musi być objęte minimum **12 miesięcznym** wsparciem producenta lub producentów. Wsparcie będzie obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).
124.	Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.

125.	Interfejs użytkownika Systemu powinien być w języku polskim lub umożliwiać wgranie plików językowych tłumaczących interfejs na język polski. Musi być przejrzysty i konfigurowalny, poprzez pogrupowanie zawartości w bloki tematyczne, co ma umożliwić łatwe i szybkie wyszukiwanie odpowiednich danych.
126.	Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise", w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.
127.	Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.
128.	System powinien zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
129.	System powinien dokonywać automatycznej integracji z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach i zasobach zarejestrowanych w domenie AD, minimum to: nazwa użytkownika, login, e-mail, nazwa komputera, przynależność do grup, przełożonego, jednostkę organizacyjną oraz konta uprzywilejowane.
130.	System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
131.	System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).
132.	System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
133.	Rozwiązanie powinno posiadać funkcjonalność wysyłania powiadomień do definiowalnych grup odbiorców (co najmniej: powiadamianie email oraz SMS, opcjonalnie czat).
134.	System powinien być dostępny z poziomu dedykowanego klienta aplikacji lub obsługiwany za pomocą dowolnej przeglądarki internetowej (Chrome, Edge, Firefox), bez konieczności instalowania jakichkolwiek dodatków dla prawidłowego jego działania.
135.	System powinien umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów, które będą brane pod uwagę w ewaluacji zagrożeń.

136.	Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: a. sparsowane pola oraz ich wartości, b. listy referencyjne, c. atrybuty użytkowników z Active Directory, d. atrybuty komputerów z Active Directory, e. bazę wskaźników kompromitacji (IOC), f. informacje z elektronicznej dokumentacji, g. anomalie w zachowaniu użytkowników (UBA), h. anomalie w zachowaniu zasobów (EBA), i. podatności na zasobach, j. wyniki analizy konfiguracji, **k.** techniki MITRE ATT&CK®,
137.	System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności: a) id techniki, b) taktykę, c) platformy których dotyczy, d) potencjalne źródła, e) opis zagrożenia, f) mityzację, g) sposób detekcji, h) referencje.
138.	Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: a) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, b) segregacja – segregacja i kwalifikacja zdarzeń, c) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, d) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, e) zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.
139.	System pozwoli na prezentację danych w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.
140.	System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących: a) zestaw wykresów dla bieżącego użytkownika, b) zestaw wykresów dla wybranego użytkownika, c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

141.	System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy: a) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia: • ilość zdarzeń nowych i niesklasyfikowanych, • ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa, • ilość zdarzeń sklasyfikowanych jako fałszywe alarmy, b) wykres przedstawiający skale zagrożeń, który uwzględnia: • ilość zasobów krytycznych na których są obsługiwane zdarzenia, • ilość zasobów niekrytycznych na których są obsługiwane zdarzenia, c) wykres przedstawiający źródła zagrożeń, który uwzględnia: • ilość nowych zdarzeń dotyczących użytkowników, • ilość podjętych zdarzeń dotyczących użytkowników, • ilość nowych zdarzeń dotyczących zasobów, • ilość podjętych zdarzeń dotyczących zasobów, d) wykres przedstawiający poziom zagrożeń, który uwzględnia: • ilość nowych zdarzeń w podziale na priorytety, • ilość podjętych zdarzeń w podziale na priorytety, e) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia: • ilość zdarzeń zarejestrowanych w bieżącym dniu, • ilość zdarzeń zarejestrowanych w ostatnim tygodniu, • ilość zdarzeń zarejestrowanych w ostatnim miesiącu, • ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu, f) wykres przedstawiający zagrożone usługi, który uwzględnia: • ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, • ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia, g) wykres przedstawiający zagrożone dane, który uwzględnia: • ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, • ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, h) wykres przedstawiający skale podatności, który uwzględnia: • ilość zasobów krytycznych na których są obsługiwane podatności, • ilość zasobów niekrytycznych na których są obsługiwane podatności, i) wykres przedstawiający czas obsługi podatności, który uwzględnia: • ilość podatności zarejestrowanych w bieżącym dniu, • ilość podatności zarejestrowanych w ostatnim tygodniu, • ilość podatności zarejestrowanych w ostatnim miesiącu, • ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu, j) wykres przedstawiający wagę podatności, który uwzględnia: • ilość nowych podatności w podziale na priorytety,

	• ilość podjętych podatności w podziale na priorytety,
142.	Nawigacja w ramach „Dashboard'u" musi wspierać opcję typu „Drill down" w następującym zakresie: a) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, b) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, c) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, d) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, e) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, f) „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.
143.	System powinien automatycznie wyodrębnić konta użytkowników oraz ich kontekst, minimum przynależność do odpowiednich grup domenowych, konta serwisowe, użytkowników uprzywilejowanych, użytkowników w randze kierowniczej i zarejestrowane stacje robocze celem automatycznej dystrybucji tych danych do odpowiednich narzędzi systemu.
144.	System powinien umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
145.	Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: a. nowe zasoby wykryte w sieci, b. typy wykrytych zasobów (np.: serwer lub stacja robocza), c. zastosowane na nich zabezpieczenia, d. usługi z którymi się komunikują, e. nowe usługi wykryte na zasobie, f. komunikacje do usług wykrytych na zasobie.
146.	System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
147.	System powinien umożliwiać przechowywanie teczek incydentów zawierających dowody, próbki, logi oraz inne powiązane z danym incydentem informacje.
148.	System powinien potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody w teczkach Incydentów.

149.	System powinien umożliwiać powiązanie każdego zdarzenia/incydentu z odpowiednim priorytetem (definiowanym automatycznie z możliwością manualnej zmiany).
150.	System powinien posiadać możliwość rejestracji zgłoszeń i przekształcenia ich w incydenty bezpieczeństwa z możliwością rozdzielenia uprawnień dla obu tych czynności.
151.	System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
152.	Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.
153.	Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)
154.	Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.
155.	Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.
156.	Rozwiązanie nie może nie może wykorzystywać klasycznej relacyjnej bazy danych (tj.: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.
157.	Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.
158.	Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.
159.	Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).
160.	Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)
161.	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).
162.	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.

163.	Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości: a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej; b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; d) zdolność do monitorowania integralności plików; e) zdolność do monitorowania rejestru systemowego; f) zdolność do monitorowania urządzeń zewnętrznych (removable devices); g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS; h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS; j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.
164.	System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.
165.	Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in. a) wszystkie skorelowane zdarzenia, b) korespondencja pocztowa, c) załączniki z próbkami lub dowodami, d) wskaźniki kompromitacji (IoC), e) informacje pozyskane z innych systemów.
166.	System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.
167.	Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

168.	Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: a) identyfikację celu i źródła zagrożenia, b) nazwę oraz adres IP źródła zagrożenia, c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, d) lokalizację z które pochodzi zagrożenie np.: Internet, e) strefę bezpieczeństwa z której pochodzi zagrożenie, f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), h) nazwę oraz adres IP celu zagrożenia, i) zabezpieczenia lokalne chroniące cel zagrożenia, j) strefę bezpieczeństwa w której znajduje się cel zagrożenia.
169.	Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).
170.	Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.
171.	Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: a) nazwy zasobu, b) rodzaju zasobu, c) ważności zasobu dla organizacji, d) rodzaj przetwarzanych informacji, e) usług, które ten zasób świadczy, f) lokalizację użytkowników, którzy z niego korzystają, g) usługi z których zasób korzysta
172.	System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

173.	System powinien umożliwiać grupowanie manualne w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
174.	System powinien grupować automatycznie w jeden incydent bezpieczeństwa zdarzenia podobne/powiązane np. wielokrotnie raportowane, przez systemy źródłowe, wielokrotnie zgłoszone przez użytkowników.
175.	System powinien umożliwiać obsługę tzw. lawinowych incydentów (incydenty takie same, lecz pochodzące od różnych użytkowników lub systemów) poprzez podłączanie ich do jednego głównego incydentu oraz nadanie odpowiedniego priorytetu tego typu zdarzeniom. Zamkniecie głównego incydentu/zdarzenia powinno umożliwiać zamykanie powiązanych z nim incydentów/zdarzeń w trybie manualnym (operator) lub automatycznym (system). W podglądzie incydentu powinna się pojawić informacja o podpiętych incydentach.
176.	System powinien pozwalać na określenie automatycznych oraz inicjowanych przez operatora reakcji na incydenty bezpieczeństwa i/lub zdarzenia, polegających na integracji z systemami zewnętrznymi w celu uzyskania dodatkowych informacji, dotyczących incydentu/zdarzenia lub podjęcia akcji zapobiegawczych.
177.	W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: a. podgląd aktywności zagrożonego zasobu na linii czasu, b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, e. w przypadku wykrytej techniki Mitre ATT@CK jej szczegółowy opis, f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, g. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o: • listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, • listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym, h. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o: • listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, • listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.
178.	System powinien umożliwiać wykonywanie działań remediacyjnych na stacjach roboczych/serwerach (pobieranie logów, uruchamianie skryptów, weryfikacja rejestrów, itp.).
179.	System powinien umożliwiać przypisywanie i przekazywanie incydentów do operatorów lub grup operatorów
180.	System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub/i PowerShell), na skonfigurowanie nowych, nie uwzględnionych przez producentów rozwiązania możliwości integracyjnych z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.
181.	System powinien umożliwiać przeglądanie listy zasobów (urządzeń, systemów, osób, itp.) pod kątem poziomu i ilości incydentów, które są z nimi powiązane.

182.	System powinien mieć możliwość automatycznego informowania o zmianie statusu incydentu (mpythoninimum: wygenerowaniu, przypisaniu, przekroczeniu czasu SLA oraz zamknięciu karty incydentu).
183.	System powinien umożliwiać ustawienie parametrów SLA bazując na ustalonym automatycznie priorytecie zdarzania/incydentu/podatności. System powinien dokonywać automatycznego pomiaru tych czasów i weryfikacji ich do zdefiniowanych wymagań SLA. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu.
184.	System powinien umożliwiać dodawanie, modyfikację i usuwanie umów SLA, które zawierają co najmniej następujące parametry: data rozpoczęcia i zakończenia obowiązywania umowy, jednostka organizacyjna (struktura jednostek), której dotyczy umowa, lista usług z katalogu usług, których dotyczy umowa.
185.	System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach: a) przekroczenia czasu reakcji o określony czas np.: o godzinę, b) możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, c) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, d) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, e) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, f) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, g) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, h) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, i) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, j) przekroczenia czasu reakcji dla podatności na zasobie krytycznym, k) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,
186.	Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na: a) wybór raportu który ma zostać wysłany, b) zdefiniowanie jego tytułu, c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d) możliwość ograniczenia cyklu do dni powszednich, e) określenie daty przesłania pierwszego raportu, f) określenie okresu przez jaki będą one przesyłane, poprzez: • zdefiniowanie daty końcowej, • bez daty końcowej, • określenie liczby raportów, g) określenie odbiorców raportu

187.	Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a) warunki powiadomień, • podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, • podatności o przekroczonych czasach SLA o definiowalny okres, • podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, • podatności, których priorytet osiągnął określoną wartość, • zdarzeń realizujących zdefiniowaną usługę, • zdarzeń przetwarzających sklasyfikowane informację, • zdarzeń przetwarzanych na krytycznych zasobach, b) odbiorców powiadomień, w tym: • operatora, któremu została przydzielona podatność, • właściciela zasobu na którym wystąpiła podatność, • zespół obsługi, który odpowiada za obsługę podatności, • właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność, • podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną. c) kanały powiadomień, m.in. e-mail, sms, komunikator, d) zastosowanie mechanizmów grupowania: • grupowanie wielu powiadomień w jednej wiadomości, • ograniczenie liczby wierszy powiadomienia do określonej wartości.
188.	System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a) przydzielenia nowej podatności do obsługi z określonym priorytetem, b) przydzielenia nowej podatności do obsługi na zasobie krytycznym, c) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, d) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, e) modyfikacji przydzielonej operatorowi podatności przez innego operatora, f) zamknięcia przydzielonej operatorowi podatności przez innego operatora, g) przejęcia przydzielonej operatorowi podatności przez innego operatora.
189.	System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a) utworzenia nowego zdarzenia z określonym priorytetem, b) utworzenia nowego zdarzenia na zasobie krytycznym, c) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, d) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, e) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, f) modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, g) zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, h) przejęcia przydzielonego operatorowi zdarzania przez innego operatora.

190.	System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
191.	Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne ze słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
192.	Interfejs modułu obsługi incydentów musi prezentować listę podatności zasobów związanych z incydentem.
193.	System powinien automatycznie ustalać priorytety podatności w odniesieniu do ważności podatnych systemów IT dla organizacji oraz oceny technicznej zagrożenia bazującej na wartości CVSS lub wartości pozyskanej bezpośrednio z silnika skanera.
194.	Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: a) wyliczonym priorytecie podatności, b) aktualnym statusie obsługi, c) ważności zasobu na którym została wykryta, d) adresie IP tego systemu, e) parametrów SLA związanych z tym statusem, f) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, g) parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”.
195.	System powinien uwzględniać w ocenie zdarzeń i incydentów, informacje o podatnościach technicznych wykrytych przez narzędzia do zarządzania podatnościami zarówno przez import raportu jak i integrację przez API.
196.	System powinien zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamiać procesy skanowania i analizowania uzyskanych raportów.
197.	System powinien umożliwiać obsługę podatności w ramach scenariuszy obsługi (playbook).
198.	Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.
199.	Produkt musi umożliwiać równoczesną pracę co najmniej 3 operatorów oraz obsługiwać 100 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.
200.	Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

201.	System ma gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.
202.	System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
203.	Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów od chwili podpisania protokołu odbioru. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).
204.	Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.
205.	Po zakończonym wdrożeniu należy zapewnić bezpłatne 3-dniowe certyfikowane szkolenia (3 x 8h) w zakresie użytkowania i administrowania wdrożonego systemu lub systemów dostarczonych w ramach zamówienia. Szkolenie ma zostać przeprowadzone dla minimum 1 osoby i uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządzanie incydentami bezpieczeństwa; kompletowanie informacji potrzebnych do opracowania raportu o incydencie; szacowanie ryzyka itp.). Szkolenia muszą być zakończone certyfikatem potwierdzającym wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej. Szkolenia muszą być przeprowadzone w języku polskim.
206.	Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji w języku polskim (tj. dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).
207.	Zmawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu dwóch dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona.

Wymagania dla pkt 3

Dostawa i wdrożenie oprogramowania do monitorowania i zarządzania siecią

Wymagania ogólne dla systemu zarządzania

- Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
- Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
- Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
- Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
- Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
- Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
- Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
- Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
- Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
- Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
- Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
- Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
- Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
- Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.

- Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).
- Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
- Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
- Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
- Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
- Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
- Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
- Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
- Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
- Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
- Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
- Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
- Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu,

obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).

- Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
- Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
- Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
- Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

- Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
- Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
- Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
- Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
- Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
- Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
- Oprogramowanie musi umożliwiać analizę sprzętową:

  - płyty głównej w zakresie model, producent, nr. seryjny,
  - CPU w zakresie nazwy, modelu, producenta, częstotliwości,
  - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
  - RAM w zakresie wielkości pamięci,
  - karty sieciowej w zakresie model, adres IP, adres MAC,
  - karty graficznej w zakresie model.

- Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
- Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
- Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
- Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
- Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
- Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
- Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
- Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
- Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
- Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

- Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
- Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
- Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
- Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
- Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
- Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
- Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.

- Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
- Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
- Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania

- Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
- Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych
- w procesie automatycznego audytu licencji (rozliczenie ilościowe).
- Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
- Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
- Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

CMDB

- Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
- Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
- Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
- Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
- Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI
- Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
- Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej oraz graficznej
- Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji

- Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy usługami, sprzętem, organizacją oraz pracownikami
- Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
- Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
- Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
- Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
- Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
- Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

Zarządzanie zasobami oraz użytkownikami

- Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
- Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
- Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
- Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
- Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
- Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
- Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.
- Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.
- Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.

- Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
- Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
- Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF
- Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
- Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
- Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
- Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
- Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
- Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
- Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
- Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
- Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami
- Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
- Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
- Oprogramowanie musi udostępniać kreator raportów dla zasobów
- Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu
- Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
- Oprogramowanie musi umożliwiać ewidencję magazynów
- Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
- Oprogramowanie musi umożliwiać ewidencję produktów magazynowych
- Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
- Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
- Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn
- Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
- Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
- Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM

- Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
- Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
- Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
- Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
- Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
- Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
- Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami
- Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

Zdalny pulpit, zdalne zarządzanie komputerem

- Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
- Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
- Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
- Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
- Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
- Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
- Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
- Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
- Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.

- Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
- Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
- Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
- Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
- Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
- Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
- Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
- Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja

- Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
- Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
- Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
- Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
- Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
- Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.

- Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
- Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
- Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
- Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
- Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
- Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
- Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
    - Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
    - Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
    - Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
    - Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
    - Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
    - W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.

- Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
- Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
- Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
- Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
- Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
- Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
- Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
- Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

Backup danych użytkownika

- Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
- Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
- Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
- Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
- Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
- Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
- Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.
- Zarządzanie urządzeniami USB Storage
- Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.

- Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
- Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
- Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
- Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Monitoring stanowisk komputerowych

- Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
- Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
- Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
- Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
- Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
- Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
- Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
- Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
- Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
- Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
- Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
- Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
- Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
- Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB.

Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.

- Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.
- Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

ServiceDesk – Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:

- Zarządzanie problemem
- Zarządzanie incydentem
- Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
- Zarządzanie umowami serwisowymi
- Definicje poziomów SLA (reakcja, naprawa, reklamacja)

- Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania iinnych typów awarii zdefiniowanych przez administratora.
- Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.
- Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
- Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
- Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
- Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
- Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
- Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
- Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
- Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.

- Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
- Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
- Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
- Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
- Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
- Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
- Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
- Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
- Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
- Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
- Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja awarii komputera).
- Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
- Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.

- Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
- Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
- Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
- Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
- Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
- Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji
- mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
- Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
- Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
- Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
- Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
- Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:

  - Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
  - Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
  - Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
  - Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
  - Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
  - Zamykanie zgłoszenia po upływie czasu reklamacji.
  - Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
  - Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
  - Walidacja zamkniętych zadań w zamykanym zgłoszeniu.

- Systemowe potwierdzanie realizacji zgłoszenia.
- Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.

- Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
- Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
- Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
- Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
- Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
- Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
- Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
- Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem
- Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
- Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
- Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
- Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
- Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
- Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
- Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
- Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
- Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
- Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.

- Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora.
- Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
- Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.
- Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
- Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
- Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
- Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.
- Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
- Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
- Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
- Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
- Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

ServiceDesk – Zarządzanie wnioskami

- Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
- Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
- Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

ServiceDesk – Zarządzanie uprawnieniami

- Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych

- Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
- Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
- Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
- Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
- Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
- Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
- Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
- Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

ServiceDesk – Zarządzanie rezerwacjami

- Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
- Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
- Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
- Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
- Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
- Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

Monitoring sieci LAN

- Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony

- Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
- Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
- Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
- Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
- Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

Zarządzanie dokumentami

- Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
- Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
- Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
- Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
- Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników
- Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym
- Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
- Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany

System wewnętrznego komunikatora dla użytkowników

- Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.

- Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostrgeSQL
- Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
- Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
- Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
- Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.
- Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
- Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
- Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
- Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
- Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
- Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
- Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
- Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania Dodatkowe:

- **Dostarczone licencje na oprogramowanie muszą być bezterminowe.**
- Dostarczone licencje na oprogramowanie muszą być dostarczone z min **18 miesięcznym supportem** producenta, liczonym od daty zakończenia wdrożenia.
- Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
- Dostarczone licencje na oprogramowanie muszą objąć co najmniej 60 stanowisk komputerowych z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np.

drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencji dostępowej do konsoli zarządzającej

- W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.
- Zamawiający wymaga od wykonawcy, aby w terminie 20 dni od podpisania umowy przeprowadził wdrożenie systemu zdalnie (wymagana co najmniej 1 sesja – 5 godzinna).