



Fundusze Europejskie
dla Podkarpacia



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



PODKARPACKIE
przestrzeń otwarta

Zamawiający:

GMINA SKOŁYSZYN

38-242 Skołyszyn 12

tel. /fax 13 4491062-64

e-mail: przetargi@skolyszyn.pl; gmina@skolyszyn.pl

strona internetowa: <https://bip.skolyszyn.pl>

Skołyszyn, styczeń 2025 r.

Załącznik nr 1
Szczegółowy opis przedmiotu zamówienia

Nr postępowania: GPIR.271.5.1.2025

Zamówienie realizowane w ramach projektu „Platforma e-usług publicznych w Gminie Skołyszyn” dofinansowanego z programu Fundusze Europejskie dla Podkarpacia 2021 – 2027 priorytetu FEPK.01 Konkurencyjna i Cyfrowa Gospodarka / działania FEPK.01.02 Cyfryzacja Numer naboru FEPK.01.02-IZ.00-001/23

GMINA SKOŁYSZYN

38-242 Skołyszyn 12

tel./fax 13 44 910 62 (63) (64)

NIP 685-16-51-203 REGON 370440382

BS O/ Skołyszyn

76 8627 1037 2003 5000 0459 0001

Spis treści

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.....	3
2. Wymagania gwarancyjne.....	3
3. Miejsce instalacji sprzętu i oprogramowania/systemu.....	4
4. Zestawienie zakresu dostaw i usług.....	5
4.1. Zestawienie zakresu dostaw i usług – część 1.	5
4.2. Zestawienie zakresu dostaw i usług – część 2.	5
4.3. Zestawienie zakresu dostaw i usług – część 3.	5
5. Szczegółowy opis pozycji – część 1.	6
5.1. Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – licencja szt. 1 – wymagania minimalne.....	6
5.2. Oprogramowanie do zarządzania infrastrukturą IT – licencja szt. 1 – wymagania minimalne.....	19
5.3. Oprogramowanie antywirusowe – licencja szt. 60 – wymagania minimalne.....	37
5.4. Oprogramowanie domenowe – licencja szt. 3 – wymagania minimalne.....	42
5.5. Oprogramowanie do backupu – licencja szt. 1 – wymagania minimalne.....	45
5.6. Oprogramowanie do wirtualizacji – licencja szt. 1 – wymagania minimalne	49
5.7. Monitoring wejść wyjść - kontrola dostępu – szt. 1 – wymagania minimalne	50
5.8. Podłoga techniczna – szt. 1 – wymagania minimalne	50
5.9. Przetąacznik sieci LAN – szt. 2 – wymagania minimalne	51
5.10. Firewall - klaster – szt. 1 – wymagania minimalne	53
5.11. Centralny system logów – szt. 1 – wymagania minimalne	58
5.12. Centralny UPS – szt. 1 – wymagania minimalne	59
5.13. Instalacja i konfiguracja (Platforma sprzętowa) – wymagania minimalne	62
6. Szczegółowy opis pozycji – część 2.	74
6.1. Agregat – szt. 1 – wymagania minimalne	74
7. Szczegółowy opis pozycji – część 3.	75
7.1. Zestaw komputerowy z oprogramowaniem – szt. 20 – wymagania minimalne	75
7.2. Laptopy – szt. 12 – wymagania minimalne.....	82

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być zgodna z normami UE i przeznaczona na rynek UE, musi również posiadać certyfikat UE lub równoważny dokument z którego wynika, że przedmiot zamówienia spełnia wymogi bezpieczeństwa i ochrony zdrowia oraz został dopuszczony do obrotu i używania na terenie Polski, zgodnie z obowiązującymi przepisami prawa
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

2. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Minimalny okres gwarancji – 5 lat;
- Gwarancja producenta z pozostawieniem dysków u Zamawiającego w przypadku ich uszkodzenia;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

Oprogramowanie

- oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);
- gwarancja nie obejmuje kosztów bieżącego utrzymania (opieka serwisowa, upgrade systemów, wersji, prawa do aktualizacji) wdrożonego oprogramowania po okresie realizacji projektu.
- Oprogramowanie musi być zarejestrowane na Gminę Skołyszyn. Dostawca oprogramowania przekaże odpowiedni certyfikat licencyjny lub inny dokument, który jednoznacznie potwierdzi taką rejestrację, ilość pozyskanych licencji oraz okres obowiązywania gwarancji.
- W ramach dostarczonych licencji przez Wykonawcę Zamawiający musi mieć możliwość korzystania ze wsparcia technicznego producenta oprogramowania na okres 60 miesięcy od daty dostawy/instalacji do Zamawiającego,
- Wszystkie dostarczane licencje muszą pochodzić z legalnego kanału dystrybucyjnego oraz muszą być objęte gwarancją i serwisem producenta na terenie Rzeczypospolitej Polskiej.
- Wykonawca, który powołuje się na rozwiązania równoważne z opisywanym przez Zamawiającego, ma obowiązek udowodnić w ofercie, że proponowane oprogramowanie spełnia kryteria równoważności. W tym celu należy dołączyć do oferty oddzielny dokument, w którym Wykonawca udowodni na swój koszt i swoją odpowiedzialność, że oprogramowanie spełnia kryteria równoważności,
- Równoważność oznacza, że:



- oprogramowanie równoważne musi być kompatybilne i w sposób niezaktócony współdziałać z oprogramowaniem posiadanym przez Zamawiającego i sprzętem funkcjonującym u Zamawiającego;
 - oprogramowanie równoważne musi zapewniać co najmniej pełną funkcjonalność oprogramowania w stosunku do którego jest wskazywane przez Wykonawcę jako równoważne i posiadać co najmniej takie same parametry techniczne i funkcjonalne;
 - warunki i zakres licencji oprogramowania równoważnego w każdym aspekcie licencjonowania muszą być nie gorsze niż licencje oprogramowania wskazanego przez Zamawiającego w stosunku do którego są równoważne;
- W przypadku zaoferowania oprogramowania równoważnego Wykonawca zobowiązany jest do przeprowadzenia minimum 3 dniowych, 8 godzinnych warsztatów szkoleniowych dla minimum 2 administratorów, z zakresu konfiguracji i administrowania oferowanym oprogramowaniem. Szkolenie musi zostać przeprowadzone w formie tradycyjnej przez producenta danego systemu lub certyfikowanego trenera.

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

3. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w budynkach urzędu lub w miejscach wskazanych przez Zamawiającego na terenie Gminy Skotyszyn.

4. Zestawienie zakresu dostaw i usług.

4.1. Zestawienie zakresu dostaw i usług – część 1.

Lp.	Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.	Wymagana minimalna długość gwarancji (m-ce)	Typ/Rodzaj gwarancji	Ilość	Jednostka miary
1.	Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa	60	Producenta/ Wykonawcy	1	lic.
2.	Oprogramowanie do zarządzania infrastrukturą IT	60	Producenta/ Wykonawcy	1	lic.
3.	Oprogramowanie antywirusowe	60	Producenta/ Wykonawcy	60	lic.
4.	Oprogramowanie domenowe	Nd	Nd	3	lic.
5.	Oprogramowanie do backupu	60	Producenta/ Wykonawcy	1	lic.
6.	Oprogramowanie do wirtualizacji	60	Producenta/ Wykonawcy	1	lic.
7.	Monitoring wejść wyjść - kontrola dostępu	60	Producenta/ Wykonawcy	1	szt.
8.	Podłoga techniczna	60	Producenta/ Wykonawcy	1	szt.
9.	Przetacznik sieci LAN CORE	60	Producenta/ Wykonawcy	2	szt.
10.	Firewall - klaster	60	Producenta/ Wykonawcy	1	szt.
11.	Centralny system logów	60	Producenta/ Wykonawcy	1	szt.
12.	Centralny UPS	60	Producenta/ Wykonawcy	1	szt.
13.	Instalacja i konfiguracja (Platforma sprzętowa)	60	Wykonawcy	150	Rbh

4.2. Zestawienie zakresu dostaw i usług – część 2.

Lp.	Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.	Wymagana minimalna długość gwarancji (m-ce)	Typ/Rodzaj gwarancji	Ilość	Jednostka miary
1.	Agregat	60	Producenta/ Wykonawcy	1	szt.

4.3. Zestawienie zakresu dostaw i usług – część 3.

Lp.	Nazwa środka trwałego lub wartości niematerialnych i prawnych itp.	Wymagana minimalna długość gwarancji (m-ce)	Typ/Rodzaj gwarancji	Ilość	Jednostka miary
1.	Zestaw komputerowy z oprogramowaniem	60	Producenta/ Wykonawcy	20	szt.
2.	Laptopy	60	Producenta/ Wykonawcy	12	szt.



5. Szczegółowy opis pozycji – część 1.

5.1. Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – licencja szt. 1 – wymagania minimalne

System przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.

1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2. System musi zapewnić agentów XDR na stacje końcowe umożliwiających im pobieranie pełnych danych telemetrycznych hostów których chronią i przestanie tych danych do systemu centralnego w celu dalszej korelacji i analizy behawioralnej. W przypadku wykrycia zagrożenia agenci muszą umożliwiać automatyczną i dostosowaną do kontekstu reakcję, m.in. na blokowanie bądź izolację sieciową złośliwego oprogramowania.
 - 2.1. Agent musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla obejmując m.in. blokowanie i odblokowywanie poszczególnych procesów bądź reguł dotyczących ruchu sieciowego stanowiące reakcję na wykryte zagrożenie.
 - 2.2. Agent musi pobierać oraz aktualizować na bieżąco listę zainstalowanego oprogramowania.
 - 2.3. System w przypadku wykrycia techniki ataku ukierunkowanego na podatną aplikację w celu zablokowania ataku musi umożliwiać zatrzymanie procesu aplikacji oraz zapewnić dostęp do danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą złośliwy proces wraz parametrami i znacznik czasowy.
 - 2.4. System musi obsługiwać scenariusz uwzględniający ocenę prawdopodobieństwa materializacji się wykrytego zagrożenia, gdzie w przypadku gdy wyliczone przez system prawdopodobieństwo ataku jest wysokie proces zostanie zablokowany, natomiast w pozostałych przypadkach gdy jest ono średnie bądź niskie zostanie on zamrożony z możliwością ponownego wznowienia przez operatora.
 - 2.5. System musi posiadać możliwość dostosowania reakcji na zagrożenie w zależności od rodzaju zasobu który chroni, przykładowo jeżeli zagrożenie dotyczyć będzie procesu na stacji roboczej proces zostanie automatycznie zablokowany jednakże w przypadku gdy to samo zagrożenie dotyczyć będzie serwera świadczącego usługi w sieci publicznej proces pozostanie uruchomiony z jednoczesną blokadą publicznego ruchu przychodzącego.
3. 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;
4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
6. 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.
7. Proces normalizacji musi 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.
8. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
10. 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.

11. 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 „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
12. 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.
13. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości 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.
15. 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 zapewnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
16. 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.
17. 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.
18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralności danych.
20. 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.
21. 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.
22. 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.
23. 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.
24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
 25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.
 26. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
 27. System musi 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.
 28. 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. komunikację do usług wykrytych na zasobie.
 29. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
 30. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
 31. 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.
 32. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz 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.
 33. 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/>).
 34. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączyjących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).
 35. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).
 36. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.
 37. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej



- synchronizacji z usługą katalogową Microsoft Active Directory.
38. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwany wynik analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).
 39. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
 40. 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.
 41. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z 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.
 42. 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.
 43. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
 44. 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).
 45. 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.
 46. 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).
 47. 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.
 48. System musi 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).
 49. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
 50. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub

- pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
51. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. 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®,
 52. 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 przestanych danych w zadanym okresie czasu,
 - g. wykrycie chwilowego wzrostu ilości przestanych danych (tzw. peek) w stosunku do całkowitej ilości przestanych danych w zadanym okresie czasu,
 - h. wykrycie sumarycznego wzrostu przestanych 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.
 53. 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^[1] (np.: proces i obraz pliku z którego został uruchomiony),
 - d. wykrycie niewystąpienia pary wartości na wybranej liście
 - e. (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).
 54. 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.
 55. 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.
- 56. 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;
- 57. 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.
- 58. 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 przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
 - d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
- 59. 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 przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
 - d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
- 60. 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 posiadających krytyczne podatności,
 - d. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.
- 61. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:
 - a. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiające 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.
- 62. 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.
- 63. 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.
64. 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.
65. 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.
66. 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.
67. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.
68. 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.
69. 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 rozdzielania 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.
70. 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.
71. 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 której 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.
72. 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 przetwarzania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).
 73. 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.
 74. 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.
 75. 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.
 76. 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. zdarzenie obsłużone – zdarzenie, które zostało obsłużone w systemie.
 77. 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”.
 78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.
 79. 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.
 80. 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.
81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
 82. 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 obsługiwanym zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.
 83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji 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.
 84. 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 rozszerzające 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 rozszerzające 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.
 85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
 - a. warunki powiadomień,
 - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
 - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - zdarzeń, których priorytet osiągnął określoną wartość,
 - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
 - zdarzeń na których doszło do naruszenia bezpieczeństwa,
 - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
 - zdarzeń realizujących zdefiniowaną usługę,
 - zdarzeń przetwarzających sklasyfikowane informacje,
 - zdarzeń przetwarzanych na krytycznych zasobach,
 - b. odbiorców powiadomień, w tym:
 - operatora, któremu zostało przydzielone zdarzenie,
 - właściciela zasobu na którym wystąpiło zdarzenie,
 - zespół obsługi, który odpowiada za obsługę zdarzeń,
 - właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
 - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego 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.
 86. 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:
- utworzenia nowego zdarzenia z określonym priorytetem,
 - utworzenia nowego zdarzenia na zasobie krytycznym,
 - utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
 - utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
 - utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
 - modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
 - zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
 - przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.
87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:
- wybór raportu, który ma zostać wysłany,
 - zdefiniowanie jego tytułu,
 - zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
 - możliwość ograniczenia cyklu do dni powszednich,
 - określenie daty przestania pierwszego raportu,
 - możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:
 - zdefiniowanej daty końcowej,
 - określonej liczby raportów,
 - określenie odbiorców raportu.
88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).
89. 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 wyznaczają dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:
- strefę bezpieczeństwa w której została wykryta podatność,
 - prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
 - rodzaj zasobu którego dotyczy ta podatność,
 - ważność tego zasobu dla organizacji,
 - przetwarzane na tym zasobie informacje, np.: dane osobowe,
 - usługi realizowane przez ten zasób, np.: DNS,
 - wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
 - poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
 - 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.
90. 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 jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:
- wyliczonym priorytecie podatności,
 - aktualnym statusie obsługi,
 - ważności zasobu na którym została wykryta,
 - adresie IP tego systemu,
 - parametrów SLA związanych z tym statusem,
 - przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
 - parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV)” = „Network”.
92. 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:
- 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,
93. 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 informacje,
 - 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 obsługiwany 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.
94. 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.
95. 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 wysłany, np.: tygodniowy lub miesięczny,
 - d. możliwość ograniczenia cyklu do dni powszednich,
 - e. określenie daty przestania pierwszego raportu,
 - f. określenie okresu przez jaki będą one przesyłane, poprzez:
 - zdefiniowanie daty końcowej,
 - bez daty końcowej,



- określenie liczby raportów,
 - g. określenie odbiorców raportu.
96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentację danych do potrzeb zalogowanego użytkownika.
97. 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).
98. 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 skalę 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,
 - 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,
 - g. wykres przedstawiający skalę podatności, który uwzględnia:
 - ilość zasobów krytycznych na których są obsługiwane podatności,
 - ilość zasobów niekrytycznych na których są obsługiwane podatności,
 - h. 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,
 - i. wykres przedstawiający wagę podatności, który uwzględnia:
 - ilość nowych podatności w podziale na priorytety,



- ilość podjętych podatności w podziale na priorytety,
99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:
 - a. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obudowie 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.
 100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
 101. 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.
 102. 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 funkcjonalnościami będzie mógł je potwierdzić lub im zaprzeczyć.
 103. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.
 104. 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 licencja nie może nakładać limitów w tym zakresie.
 105. Produkt musi umożliwiać równoczesną pracę co najmniej 5 operatorów oraz obsługiwać 200 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.
 106. Dla wszystkich źródeł objętych licencją oraz stanowiących jednocześnie komputery bądź serwery licencja produktu musi uwzględniać możliwość wykorzystania dedykowanych agentów XDR.
 107. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
 108. 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.
 109. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
 110. Dostarczone rozwiązanie musi być objęte wsparciem producenta lub producentów. 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).

111. Wykonawca udzieli Zamawiającemu wieczystej (perpetual), nieograniczonej czasowo licencji na zakupiony System.

5.2. Oprogramowanie do zarządzania infrastrukturą IT – licencja szt. 1 – wymagania minimalne

1. Architektura / budowa
 - 1.1. Licencja bezterminowa na oprogramowanie powinna objąć wszystkie stanowiska komputerowe z 60 miesięcznym wsparciem serwisowym.
 - 1.2. System musi posiadać następującą architekturę:
 - 1.2.1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
 - 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).
 - 1.2.3. Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.
 - 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
 - 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
 - 1.2.6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
 - 1.2.7. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.
 - 1.2.8. Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.
 - 1.2.9. Agent musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi.
 - 1.2.10. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.
 - 1.2.11. System musi posiadać możliwość wygenerowania instalatora Agentów, który nie będzie wymagał uprawnień administracyjnych do zainstalowania.
 - 1.2.12. Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).
 - 1.2.13. System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w



sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

- 1.2.14. Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.
- 1.2.15. Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta.
- 1.2.16. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
- 1.2.17. System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.
- 1.2.18. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.

2. Wymagania systemowe

- 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).
- 2.2. Agent musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
- 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11.
- 2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
- 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
- 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

- 3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usług MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- 3.2. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
- 3.3. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.
- 3.4. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.
- 3.5. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switchy itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, dacie zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z



- wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.
- 3.6. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.
4. Funkcjonalności systemu zarządzania infrastrukturą IT
- 4.1. Funkcjonalność agenta
- 4.1.1. System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączenia agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączenia polityk w obszarze bezpieczeństwa (DLP).
- 4.1.2. Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość
- 4.1.3. Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkownika, który go wyświetlił.
- 4.1.4. Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agentu.
- 4.1.5. Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania.
- 4.2. Funkcjonalność konsoli administracyjnej.
- 4.2.1. Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersję angielską.
- 4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).
- 4.2.3. Konsola administracyjna musi posiadać dashboards – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.
- 4.2.4. Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu.
- 4.2.5. Dashboard prezentujący parametry sieci zawiera widżety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.
- 4.2.5.1.1. Lista monitorowanych usług: AIM/ICQ, Back Orifice, Bagle.B, Bagle.h, BGMP, BGP, BitTorrent, Blaster, Blizzard's Battle.net, Call of Duty, Dabber, DHCPv6 (client), DHCPv6 (server), Direct Connect, DNS, Doom, Emule, FTP (connection control), FTP (data port), FTPS (TLS/SSL)(connection control), FTPS (TLS/SSL)(data port), GameSpy Arcade, Gnutella, Gopher protocol, HTTP, HTTP Proxy, HTTPS, IMAP, IMAPS, IMAPv3, iperf, IRC, IRC, iSCSI, Jedi Knight: Jedi Academy, Kazza, Kerberos, Killing Floor, LDAP, LDAP (SSL), LDP, LogMeIn Hamachi, MMP, MPP, MS Exchange Routing, MS Media Server, MS SQL Server (monitor), MS SQL Server (server), MSDP, MSN, Mu Online, Mxit, MySQL, Nessus, NetBIOS (Datagram Service), NetBIOS (Name Service), NetBIOS (Session Service), NetBus, NFS, Niektóre gry firmy Blizzard, Nintendo Wi-Fi Connection, NNTP, NNTP (TLS/SSL), NTP, OpenVPN, POP3, POP3S, PostgreSQL, PPTP, Printer-IPP, Printer-RAW, Print-spooler, Radio internetowe, Rbot/Spybot, RDP, rsyncs, RTCP, RTP, RTSP, Sasser, SFTP, SIP, SIP(TLS), SLP, SMB, SMTP, SMTPS, SNMP, SOCKS proxy, SSH, Steam, Structured Query Language (SQL) Services, Sub7, Symantec System Center agent, TACACS, TeamViewer, Telenet (TLS/SSL), Telnet, TSP, UUCP, VMware Server, VMware VAMI, WASTE, WHOIS, WINS, XMPP/Jabber, Yahoo!, Messenger.
- 4.2.5.1.2. Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.



- 4.2.6. Dashboard prezentujący informacje o bezpieczeństwie zawiera widżety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez bitlockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez agenta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych, nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cał, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie cpu, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.
- 4.2.7. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.
- 4.2.8. Dane na widżetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika.
- 4.2.9. Widżety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widżetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widżety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)
- 4.2.10. Z każdego widżetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widżecie).
- 4.2.11. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.
- 4.2.12. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).
- 4.2.13. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.
- 4.2.14. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.
- 4.2.15. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
- 4.2.16. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.
- 4.2.17. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).
- 4.2.18. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.



- 4.2.19. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).
- 4.2.20. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)
- 4.2.21. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.
- 4.3. Funkcjonalność panelu pracownika
 - 4.3.1. Automatyczne uruchamianie panelu w momencie zalogowania użytkownika do systemu operacyjnego.
 - 4.3.2. Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.
 - 4.3.3. Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.
 - 4.3.4. Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidualnego bądź grupowego włączania / wyłączenia (ukrywania) sekcji.
 - 4.3.5. Sekcje informacyjne panelu pracownika
 - 4.3.5.1. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – nazwa domenowa, nr telefonu, nr telefonu komórkowego, stanowisko
 - 4.3.5.2. Dashboard
 - 4.3.5.2.1. Mój komputer – wykorzystanie RAM, dysku, CPU.
 - 4.3.5.2.2. Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi.
 - 4.3.5.3. Sprzęt
 - 4.3.5.3.1. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
 - 4.3.5.3.2. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
 - 4.3.5.3.3. Urządzenia przypisane przez pracownika (nr seryjny, typ, IP).
 - 4.3.5.3.4. Urządzenia używane przez pracownika (nr seryjny, typ, IP).
 - 4.3.5.4. Oprogramowanie
 - 4.3.5.4.1. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie 2 okresi ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).
 - 4.3.5.5. Wiadomości
 - 4.3.5.5.1. Lista wiadomości przesłanych do użytkownika (data, typ wiadomości, nadawca, treść).
 - 4.4. Zarządzanie licencjami
 - 4.4.1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).
 - 4.4.2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.
 - 4.4.3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.
 - 4.4.4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania”, które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe” – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe” - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone” – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.
 - 4.4.5. System umożliwia zdefiniowanie listy aplikacji zabronionych.



- 4.4.6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).
- 4.4.7. System musi umożliwiać zdefiniowanie dowolnej kategorii oprogramowania /pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.
 - 4.4.7.1. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.
 - 4.4.7.2. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.
 - 4.4.7.3. Niezależność od zewnętrznych dostawców bazy wzorców procesów.
- 4.4.8. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).
- 4.4.9. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe.
- 4.4.10. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.
- 4.4.11. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.
- 4.4.12. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.
- 4.4.13. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.
- 4.4.14. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).
- 4.4.15. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.
- 4.4.16. System prezentuje datę instalacji oprogramowania.
- 4.4.17. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
- 4.4.18. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).
- 4.4.19. System umożliwia zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).
- 4.4.20. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.
- 4.4.21. System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności.
- 4.4.22. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.
- 4.4.23. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.
- 4.4.24. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.
- 4.4.25. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę



godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.

4.5. Wzorce aplikacji i pakietów

- 4.5.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,5 tys. wzorców aplikacji, 1,3 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania.
- 4.5.2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.
- 4.5.3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.
- 4.5.4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.
- 4.5.5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.
- 4.5.6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.
- 4.5.7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).

4.6. Inwentaryzacja sprzętu komputerowego

- 4.6.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).
- 4.6.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.
- 4.6.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
- 4.6.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
- 4.6.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza poczynawszy od wskazanego miejsca w hierarchii kluczy rejestru.
- 4.6.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
- 4.6.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
- 4.6.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
- 4.6.9. System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane).
- 4.6.10. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
- 4.6.11. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
- 4.6.12. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne).
- 4.6.13. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
- 4.6.14. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
- 4.6.15. System umożliwia dodawanie notatek do każdej pozycji sprzętu.



- 4.6.16. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
- 4.6.17. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
- 4.6.18. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkownika, likwidacja).
- 4.7. Inwentaryzacja urządzeń podłączanych do komputera
 - 4.7.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp).
 - 4.7.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
 - 4.7.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).
- 4.8. Inwentaryzacja urządzeń innych niż komputery
 - 4.8.1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switchy, routery, monitory, pamięci masowe itp.
 - 4.8.2. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/portcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.
 - 4.8.3. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
 - 4.8.4. System musi zbierać informacje o jakości połączenia:
 - 4.8.4.1. Czas odpowiedzi serwisów (usług) podawany w milisekundach:
 - 4.8.4.1.1. Średni czas odpowiedzi.
 - 4.8.4.1.2. Minimalny czas odpowiedzi.
 - 4.8.4.1.3. Maksymalny czas odpowiedzi.
 - 4.8.4.2. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.
 - 4.8.5. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.
 - 4.8.5.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
 - 4.8.5.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.
 - 4.8.6. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
 - 4.8.6.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
 - 4.8.7. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.
 - 4.8.8. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
 - 4.8.9. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
 - 4.8.10. System musi mieć możliwość przypominania o upływającym terminie gwarancji.
 - 4.8.11. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
 - 4.8.12. System udostępnia informację o wartości wprowadzonego sprzętu.
 - 4.8.13. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.
 - 4.8.14. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.
 - 4.8.15. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki



oraz umożliwiać dotarcie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

4.9. Zdalna administracja komputerami

- 4.9.1. System ma automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
- 4.9.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.
- 4.9.3. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączenie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.
- 4.9.4. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).
- 4.9.5. System musi umożliwiać za pomocą technologii Ultra VNC: przejście ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacją oprogramowania, poprawek i aktualizacji (service pack, patch).
- 4.9.6. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.
- 4.9.7. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.
- 4.9.8. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejścia dostępu).
- 4.9.9. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.
- 4.9.10. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.
- 4.9.11. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).
- 4.9.12. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. System posiada co najmniej 70 predefiniowanych poleceń.
- 4.9.13. System musi umożliwiać zdalne połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC.
- 4.9.14. System musi umożliwiać za pomocą technologii WEBRTC: przejście ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch).
- 4.9.15. System musi umożliwiać poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie) i wykorzystanie wiersza poleceń (cmd) oraz powershell bez konieczności podłączenia do komputera.
- 4.9.16. System musi umożliwiać nagrywanie sesji połączeń WEBRTC jak i nawiązywanie komunikacji z użytkownikiem podczas sesji (czat).



- 4.9.17. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
- 4.9.18. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
- 4.10. Automatyzacja
 - 4.10.1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.
 - 4.10.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.
 - 4.10.3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.
 - 4.10.4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
 - 4.10.5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,
 - 4.10.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).
 - 4.10.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
 - 4.10.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.
 - 4.10.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy /drugi /trzeci/ czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.
 - 4.10.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.
- 4.11. Zarządzanie magazynem IT
 - 4.11.1. System musi umożliwiać obsługę magazynu IT.
 - 4.11.2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.
 - 4.11.3. System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI.
 - 4.11.4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).
 - 4.11.5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.
 - 4.11.6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.
- 4.12. Repozytorium
 - 4.12.1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.



- 4.12.2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.
- 4.13. Kody kreskowe
- 4.13.1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.
- 4.13.2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.
- 4.13.3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.
- 4.13.4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.
- 4.13.5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.
- 4.13.6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.
- 4.13.7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.
- 4.13.8. Parametry kodu kreskowego (wymiały, wielkość i typ czcionki) muszą być definiowalne.
- 4.13.9. System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów.
- 4.14. System szkolenia pracowników za pomocą wiadomości.
- 4.14.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.
- 4.14.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.
- 4.14.3. Formatowanie treści musi być zgodne z HTML.
- 4.14.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
- 4.14.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
- 4.14.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualnie i dźwiękowo o otrzymaniu nowej wiadomości.
- 4.14.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
- 4.14.8. System musi posiadać zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.
- 4.14.9. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.
- 4.14.10. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
- 4.14.11. System musi posiadać możliwość eksportu / importu treści.
- 4.15. Monitorowanie drukarek sieciowych i wydruków
- 4.15.1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
- 4.15.2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
- 4.15.3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.



- 4.15.4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
- 4.15.5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.
- 4.15.6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.
- 4.15.7. Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych
- 4.16. Monitorowanie stron www
 - 4.16.1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
 - 4.16.2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
 - 4.16.3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
 - 4.16.4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.
 - 4.16.5. W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści rctstron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.
 - 4.16.6. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.
- 4.17. Monitorowanie dziennika zdarzeń
 - 4.17.1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
 - 4.17.2. Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.
 - 4.17.3. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
 - 4.17.4. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
 - 4.17.5. System musi umożliwiać monitorowanie komunikatów Syslog.
- 4.18. Monitorowanie pracy komputerów
 - 4.18.1. System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.
 - 4.18.2. System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.
 - 4.18.3. System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie
- 4.19. Monitorowanie sesji zdalnych połączeń
 - 4.19.1. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.
 - 4.19.2. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.
- 4.20. Repozytorium CMDB – centralna baza systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:



- 4.20.1. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.
- 4.20.2. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.
- 4.20.3. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.
- 4.20.4. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.
- 4.20.5. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.
- 4.20.6. Dokumenty - repozytorium dokumentów zapisanych w systemie.
- 4.20.7. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.
- 4.20.8. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.
- 4.20.9. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.
- 4.20.10. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.
- 4.20.11. Typy licencji - lista typów licencji.
- 4.20.12. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.
- 4.20.13. Typy urządzeń - lista typów urządzeń.
- 4.20.14. Urządzenia - lista urządzeń podzielonych wg typu.
- 4.20.15. Producenci / Dostawcy - lista producentów i dostawców.
- 4.20.16. Pamięć masowa - zestawienie dysków twardych z komputerów.
- 4.20.17. Porty sieciowe - lista monitorowanych portów sieciowych.
- 4.20.18. Usługi sieciowe - lista monitorowanych usług sieciowych.
- 4.20.19. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.
- 4.20.20. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.
- 4.20.21. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.
- 4.20.22. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.
- 4.20.23. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.
- 4.20.24. Serwery - lista zinwentaryzowanych serwerów.
- 4.20.25. Usługi - zestawienie usług działających na komputerach.
- 4.20.26. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.
- 4.20.27. Pamięć masowa USB - lista urządzeń pamięci masowej USB.
- 4.20.28. Administratorzy - lista administratorów systemu,
- 4.20.29. Użytkownicy / pracownicy - lista pracowników.
Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.
- 4.21. Worktime manager
 - 4.21.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.
 - 4.21.2. Dane muszą być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych.
 - 4.21.3. Dane dla grup użytkowników muszą być skumulowane oraz analityczne.
 - 4.21.4. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.



- 4.21.5. Informacje dotyczące prezentowane w panelu to informacja o otwartych sesjach, informacja o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera, informacja o aktywności użytkownika w aplikacjach, informacja o produktywności użytkownika w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.
- 4.21.6. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.
- 4.21.7. System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.
- 4.21.8. System musi posiadać widżety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.
- 4.22. Raportowanie i eksport danych
- 4.22.1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.
- 4.22.2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
- 4.22.3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
- 4.22.4. Generowanie raportu musi odbywać się po stronie serwera, a nie klienta.
- 4.22.5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).
- 4.22.6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt).
- 4.22.7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.
- 4.22.8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
- 4.22.9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.
- 4.22.9.1. Raporty z zakresu komputerów
- Komputery – Karta graficzna – Procesor
 - Komputery – Serwery wg systemu operacyjnego
 - Komputery wg procesora – Skrócony
 - Komputery wg procesora – Wszystkie
 - Komputery wg producenta – Skrócony
 - Komputery wg producenta – Wszyscy
 - Komputery wg struktur organizacyjnych – Skrócony
 - Komputery wg struktury organizacyjnej – Wszystkie
 - Komputery wg systemów operacyjnych – Skrócony
 - Komputery wg systemów operacyjnych – Wszystkie
 - Komputery wg typu – Desktop
 - Komputery wg typu – Hyper-V
 - Komputery wg typu – Mobile

- Komputery wg typu – Nieokreślone
- Komputery wg typu – Server
- Komputery wg typu – Virtual Machine
- Komputery wg typu – VMWare
- Komputery wg typu – Wszystkie typy
- Zestawienie komputerów wg typu – Skrócony
- Komputery online
- Komputery niezautoryzowane
- Komputery offline
- Komputery online
- Komputery w magazynie
- Komputery w naprawie
- Komputery wszystkie
- Komputery wycofane
- Komputery zablokowane
- Komputery zautoryzowane
- Komputery zlikwidowane
- Komputery z Intel Anti-Theft
- Komputery z Intel VPro

4.22.9.2. Raporty z zakresu urządzeń

- Urządzenia – Notatki
- Urządzenia – USB – Dodane
- Urządzenia – USB – Wykryte
- Urządzenia – USB – Wszystkie
- Urządzenia – USB – Biała lista
- Urządzenia – Serwis
- Urządzenia – Inwentaryzacja – Kody kreskowe
- Urządzenia – Inwentaryzacja
- Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji
- Urządzenia – Utrzymanie
- Urządzenia

4.22.9.3. Raporty z zakresu sieci

- Sieć – Wykryte
- Sieć – Historia
- Sieć – Ostatnie skanowanie

4.22.9.4. Raporty z zakresu oprogramowania

- Oprogramowanie – Systemy operacyjne – Wszystkie
- Oprogramowanie – Systemy operacyjne – Instalacje OEM
- Oprogramowanie – Systemy operacyjne – Szczegóły
- Oprogramowanie – Systemy operacyjne – Historia audytów
- Oprogramowanie – Aplikacje – Wszystkie
- Oprogramowanie – Aplikacje – Monitorowane
- Oprogramowanie – Aplikacje – Szczegóły
- Oprogramowanie – Aplikacje – Historia audytów
- Oprogramowanie – Pakiety – Wszystkie
- Oprogramowanie – Pakiety – Szczegóły
- Oprogramowanie – Pakiety – Historia audytów
- Oprogramowanie – Bazy danych – Wszystkie
- Oprogramowanie – Bazy danych – Express
- Oprogramowanie – Bazy danych – Pozostałe
- Oprogramowanie – Bazy danych – per Core
- Oprogramowanie – Rejestry – Razem
- Oprogramowanie – Rejestry – Szczegóły
- Oprogramowanie – Rejestry – Ostatnio zainstalowane



- Oprogramowanie – Klucze produktu
- Oprogramowanie – Wykorzystanie – Użycie – Wszystkie
- Oprogramowanie – Wykorzystanie – Oszczędności
- Oprogramowanie – Wykorzystanie – CAL
- Oprogramowanie – Wykorzystanie – CAL WEB
- Oprogramowanie – Monitorowanie – Uruchomienia
- Oprogramowanie – Monitorowanie – Aktywność ogółem
- 4.22.9.5. Raporty z zakresu osób
 - Osoby – Protokół standardowy
 - Osoby – Protokół rozszerzony
- 4.22.9.6. Raporty z zakresu plików i multimediów
 - Pliki i multimedia – Archiwa
 - Pliki i multimedia – Audio
 - Pliki i multimedia – Erotyka
 - Pliki i multimedia – Grafika
 - Pliki i multimedia – Wideo
 - Pliki i multimedia – Wykonywalne
 - Pliki i multimedia – Zmiany plików
- 4.22.9.7. Raporty z zakresu magazynu
 - Magazyn – Dokumenty
 - Magazyn – Stany
 - Magazyn – Materiały
 - Magazyn
- 4.22.9.8. Raporty z zakresu finansów
 - Finanse – Urządzenia
 - Finanse – Licencje
 - Finanse – Wydruki wg drukarki
 - Finanse – Wydruki wg sterownika
 - Finanse – Wydruki użytkownicy
 - Finanse – Magazyn
- 4.22.9.9. Raporty z zakresu serwera wiadomości
 - Serwer wiadomości – Komunikator – Historia
 - Wiadomość cykliczna – wg wiadomości
 - Serwer wiadomości – Komunikator – Rozmowy
 - Serwer wiadomości – Wiadomości wystane – wg komputera
 - Serwer wiadomości – Wiadomości wystane – wg odbiorcy
 - Serwer wiadomości – Wiadomości wystane – wg wiadomości
 - Serwer wiadomości – Wiadomości wystane – wg wysyłającego
 - Serwer wiadomości – Wiadomości – Aktywne cykle
- 4.22.9.10. Raporty z zakresu serwera monitorującego
 - Serwer monitorujący – Logowanie agentów
 - Serwer monitorujący – eServer
 - Serwer monitorujący – Alerty systemowe
 - Serwer monitorujący – Historia logowań
 - Serwer monitorujący – Dzienniki zdarzeń – Powiadomienia systemowe
 - Serwer monitorujący – Dzienniki zdarzeń – Dzienniki
 - Serwer monitorujący – Dzienniki zdarzeń – Sesje RDP
 - Serwer monitorujący – Transfer sieciowy – Procesy
 - Serwer monitorujący – Drukowanie
 - Serwer monitorujący – Drukowanie – Razem
 - Serwer monitorujący – Drukowanie – Razem SNMP
 - Serwer monitorujący – Drukowanie – Prognoza
 - Serwer monitorujący – Usługi – Wszystkie
 - Serwer monitorujący – Usługi – Szczegóły



- Serwer monitorujący – Harmonogram zadań
- Serwer monitorujący – Sesje VNC
- Serwer monitorujący – Intel AMT
- Serwer monitorujący – Strony www – Odwiedzone
- Serwer monitorujący – Strony www – Aktywność ogółem
- Serwer monitorujący – USB
- Serwer monitorujący – Wydajność – CPU
- Serwer monitorujący – Wydajność – Dysk
- Serwer monitorujący – Wydajność – Dysk (razem)
- Serwer monitorujący – Wydajność – Pamięć
- Serwer monitorujący – Wydajność – Procesy
- Serwer monitorujący – Wydajność – Sieć
- 4.22.9.11. Raporty z zakresu serwera zadań
 - Serwer zadań – Logi
 - Serwer zadań – Zadania cykliczne
- 4.22.9.12. Raporty z zakresu serwera automatyzacji
 - Serwer automatyzacji – Automaty
 - Serwer automatyzacji – Logi
- 4.22.9.13. Raporty z zakresu raportów
 - Raporty – Harmonogram
 - Raporty – Harmonogram – Historia
- 4.22.9.14. Raporty z zakresu repozytorium
 - Repozytorium – Dokumenty
 - Repozytorium – e-Learning
 - Repozytorium – Kategorie aplikacji
 - Repozytorium – Kategorie plików
 - Repozytorium – Kategorie procesów
 - Repozytorium – Kategorie www
 - Repozytorium – Producenci Dostawcy
 - Repozytorium – Typy licencji
 - Repozytorium – Zdalna instalacja – Repozytorium
 - Repozytorium – Zdalna instalacja – Logi
- 4.22.9.15. Raporty z zakresu ustawień
 - Ustawienia – Administratorzy – Wszystkie
 - Ustawienia – Dane firmy
 - Ustawienia – Struktura organizacyjna
 - Ustawienia – Budżet
 - Ustawienia – Sieci
- 4.22.10. System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.
- 4.22.10.1. Wynikiem wykonania harmonogramu jest raport w formacie pdf.
- 4.22.10.2. Harmonogram można skonfigurować.
- 4.23. Powiadomienia
 - 4.23.1. System musi umożliwiać generowanie powiadomienia w formie alertu w konsoli systemu, wiadomości email wystanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.
 - 4.23.2. System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup odbiorców
 - 4.23.3. System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.
 - 4.23.4. System musi posiadać co najmniej 30 zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych
 - 4.23.5. Powiadomienia z zakresu oprogramowania
 - Odinstalowano oprogramowanie



- Wykryto niezgodność ze schematem oprogramowania
- Wykryto nowe oprogramowanie
- 4.23.6. Powiadomienia z zakresu sieci
 - Monitorowana usługa sieciowa przestała odpowiadać
 - Monitorowane urządzenia z problemami
 - Monitorowane urządzenie jest offline
 - Problem ze stroną WWW
 - Serwis WWW nie odpowiada
 - Serwis WWW odpowiada niewłaściwym komunikatem
 - Średni czas odpowiedzi usługi przekroczył wartość X ms
 - Transfer sieciowy na komputerze przekroczył X MB / Y min
 - W sieci pojawiły się duplikaty adresów IP
 - W sieci pojawiły się duplikaty adresów MAC
 - Wykryto dużą ilość danych wysyłanych przez dany port w switch'u
 - Wykryto nowe urządzenie
 - Wykryto urządzenie z odblokowanym portem X
 - Wykryto urządzenie z usługą X
 - Wykryto zmianę adres IP komputera
 - Wykryto zmianę statusów portów w switch'u
- 4.23.7. Powiadomienia z zakresu sprzętu
 - Interfejs sieciowy wyłączony
 - Parametr lub parametry S.M.A.R.T. przekroczyły dozwolone wartości
 - Podłączono urządzenie USB
 - Wykryto zmianę w sprzęcie (WMI)
- 4.23.8. Powiadomienia z zakresu systemu
 - Mało miejsca na dysku C
 - Pojawił się błąd w dzienniku zdarzeń Windows
 - Wykryto problem z usługą systemu Windows
 - Wykryto zmianę nazwy komputera
 - Wysokie użycie pamięci RAM
 - Zmieniono informację o systemie
- 4.23.9. Powiadomienia z zakresu użytkownika
 - Użytkownik odwiedził stronę WWW z wybranej kategorii
 - Użytkownik przekroczył limit wydrukowanych stron
 - Użytkownik przekroczył transfer sieciowy X MB / Y min
- 5. Bezpieczeństwo
 - 5.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
 - 5.2. Uwierzytelnianie do systemu musi być realizowane:
 - 5.2.1. z wykorzystaniem imiennego konta użytkownika i hasła,
 - 5.2.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,
 - 5.2.3. za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory,
 - 5.2.4. za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS,
 - 5.2.5. za pomocą kluczy uwierzytelniających.
 - 5.2.6. za pomocą kodu na maila
 - 5.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.
 - 5.4. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).
 - 5.5. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.
 - 5.6. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie.

**5.7. Uwierzytelnianie za pomocą kluczy**

5.7.1. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.

5.7.2. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.

5.7.3. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.

5.8. System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.

5.9. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.

5.10. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.

5.11. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.

5.12. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).

5.13. System musi być wyposażony w mechanizmy powtórnej załadunku danych historycznych pochodzących od agentów.

5.14. System musi zapewniać:

5.14.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.

5.14.2. Przechowywanie logów systemowych.

5.14.3. Przechowywanie logów bezpieczeństwa.

5.14.4. Przechowywanie logów aktywności użytkowników i administratorów.

5.14.5. Pobieranie logów z agentów z poziomu konsoli administracyjnej.

5.14.6. Możliwość eksportu logów.

5.14.7. Definiowanie maksymalnego czasu przechowywania plików log.

5.15. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

6. Wsparcie, pomoc, informacje dodatkowe

6.1. System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinarów w języku polskim.

6.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.

6.3. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

6.4. Zdalne wykonanie instalacji, konfiguracji i profilowanie systemu.

6.5. Minimum 2 godziny szkolenia z obsługi dostarczonego systemu.

Certyfikat dla administratorów przeszkolonych z użytkowania systemu.

5.3. Oprogramowanie antywirusowe – licencja szt. 60 – wymagania minimalne**Administracja zdalna**

1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.



6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
8. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
9. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
10. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
11. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
14. Rozwiązanie musi zapewniać wystanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.



14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przetrząsnąć się w tryb pracy oparty na regułach,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
 - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
 - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze,



Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomem przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.



4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - usunięcie zawartości urządzenia,
 - przywrócenie urządzenia do ustawień fabrycznych,
 - zablokowania urządzenia,
 - uruchomienie sygnału dźwiękowego,
 - lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - nazwę aplikacji,
 - nazwę pakietu,
 - kategorię sklepu Google Play,
 - uprawnienia aplikacji,
 - pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wystanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
 - Czysty,
 - Podejrzany,
 - Bardzo podejrzany,
 - Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.



15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej możliwości podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

5.4. Oprogramowanie domenowe – licencja szt. 3 – wymagania minimalne

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie minimum 1000 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.



2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - b. Dotykowy umożliwiający sterowanie dotykaniem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
 - a. Login i hasło,
 - b. Karty z certyfikatami (smartcard),
 - c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,



- b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- c. Zdalna dystrybucja oprogramowania na stacje robocze.
- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
- e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- f. Szyfrowanie plików i folderów.
- g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- i. Serwis udostępniania stron WWW.
- j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
- k. Wsparcie dla algorytmów Suite B (RFC 4869),
- l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
 - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - Obsługi 4-KB sektorów dysków
 - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
- 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.



5.5. Oprogramowanie do backupu – licencja szt. 1 – wymagania minimalne

Wymagania ogólne

- Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 20 VM oraz 3 serwerach fizycznych.
- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
- Oprogramowanie nie może instalować żadnych statycznych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej



- Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Repozytoria oparte o XFS muszą pozwalać na niezmiennosć danych przez określoną ilość czasu (tzw Immutability)
- Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

- Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
- Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików



- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
 - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
 - BSD: UFS, UFS2
 - Solaris: ZFS, UFS
 - Mac: HFS, HFS+
 - Windows: NTFS, FAT, FAT32, ReFS
 - Novell OES: NSS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalając na odtworzenie haseł.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
- Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
- Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
- Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
- Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Monitoring

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsolę vCenter Server lub pracujące samodzielnie

- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
- System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
- System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x

Raportowanie

- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych



- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

5.6. Oprogramowanie do wirtualizacji – licencja szt. 1 – wymagania minimalne

Aktualizacja posiadanego przez Zmawiającego oprogramowania - VMW vSphere 7 ESSL Plus Kit - licencja dla 3 serwerów fizycznych posiadających 2 procesory z gwarancją utrzymania aktualnej wersji przez okres min. 2 lat.

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć
5. i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
7. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych
9. z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
11. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć min. 2 porty szeregowo.
12. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
13. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
14. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2008, Windows Server 2012, Windows 8, SLES, RHEL, Debian, CentOS, FreeBSD, Ubuntu.
15. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
16. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
17. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.



18. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
19. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
20. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
21. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
22. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączenia wirtualnych maszyn.
23. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
24. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
25. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
26. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
28. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

5.7. Monitoring wejść wyjść - kontrola dostępu – szt. 1 – wymagania minimalne

1. System kontroli dostępu do pomieszczeń serwerowych (zamek elektromechaniczny z szyfrem wejściowym) zlokalizowanych w budynku Urzędu.
2. Wymaga się, aby wszystkie przypadki dostępu były autoryzowane i sprawdzane za pomocą zabezpieczeń uwierzytelniających, takich jak karta uwierzytelniająca z czytnikiem na kod PIN.
3. System kontroli dostępu jest to zespół wzajemnie powiązanych urządzeń elektronicznych oraz mechanicznych, których działanie ma na celu ograniczenie użytkownikom (całkowite lub określonym czasie) dostępu do sektorów (stref) tego systemu. Identyfikowanie użytkowników przez system kontroli dostępu zależny jest od zastosowanego typu urządzenia identyfikującego
4. Wytyczne instalacji i uruchomienia kontroli dostępu.
5. System kontroli dostępu będzie miał osobny obwód zasilania doprowadzony z tablicy znajdującej się w serwerowni, będzie zabezpieczony zabezpieczeniem różnicowoprądowym z członom nadprądowym 2P 10A B 0,03A, obwód będzie wykonany przewodem YDYżo 3x 1,5 i powłocą polwinitowej, umieszczonym w korytach elektroinstalacyjnych.
6. Obwód zasilania będzie doprowadzony do zasilaczy buforowych z akumulatorami, z których będą zasilane czytniki kontroli dostępu k umieszczone będą przy wyznaczonych drzwiach.
7. Drzwi będą chroniły zwory elektromagnetyczne, w środku pomieszczeń będą usytuowane przyciski awaryjnego zwalniania otwarcia drzwi.
8. Czytniki kontroli dostępu będą działały na 4 cyfrowy pin utworzony indywidualnie dla każdego użytkownika.

5.8. Podłoga techniczna – szt. 1 – wymagania minimalne

1. Wykonanie podłogi teletechnicznej w istniejącym pomieszczeniu serwerowni w budynku Urzędu.
2. Podłogę techniczną o nośności zapewniającej posadowienie szaf w liczbie wynikającej z oferowanego rozwiązania sprzętowego, przy założeniu, że ciężar pojedynczej szafy wypełnionej urządzeniami wynosi maksymalnie 1000 kg.



3. Wykonawca powinien zapewnić wykonie stosownego „wjazdu” (pochylni) dla urządzeń serwerowych.
4. Przed wykonaniem prac Wykonawca jest zobowiązany do przedstawienia planu technicznego powyższych prac. Dopiero po akceptacji Zamawiającego może on przystąpić do realizacji.
5. Prace Wykonawcy nie mogą zakłócić poprawnej pracy Placówki medycznej. Wnioskodawca wymaga aby obecne urządzenia serwerowe pracowały w sposób ciągły.

5.9. Przetątnik sieci LAN – szt. 2 – wymagania minimalne

Przetątnik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów: 12 portów 10GBaseT i 12 portów SFP+ lub równoważnie 24 porty SFP+

Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:

- Gigabit Ethernet 1000Base-SX
- Gigabit Ethernet 1000Base-LX/LH
- 10Gigabit Ethernet 10GBase-SR
- 10Gigabit Ethernet 10GBase-LR
- 10Gigabit Ethernet typu twinax

Port konsoli USB Type-C/RJ45

Porty dostępowe przetątnika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:

- Przepustowość przetątnika (switching bandwidth) 480 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 240 Mpps
- Pamięć DRAM – 512 MB
- Pamięć flash – 256 MB
- Procesor wbudowany 1,3 GHz
- Wielkość bufora pakietów - 3 MB
- 2 000 grup IGMP
- 8 grupy połączeń zagregowanych typu „port channel” LACP
- 8 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
- 1 000 wpisów w listach kontroli dostępu ACL
- 8 kolejek sprzętowych

Obsługa:

- 4 000 aktywnych sieci VLAN
- 16 000 adresów MAC
- 900 statycznych tras IPv4
- 128 interfejsów L3

Obsługa ramek Ethernet Jumbo 9 000 B

Możliwość łączenia do 4 jednostek w stos poprzez porty 10 GE, zarządzane jako jeden system z funkcją failover active/standby

Funkcjonalność cross-stack QoS, VLAN, LAG i port mirroring

Przetątnik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

- IEEE 802.1w Rapid Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1s Multi-Instance Spanning Tree
- Obsługa 126 instancji protokołu STP

Funkcje wirtualnej sieci LAN: Voice VLAN, Protocol based VLAN

Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

Protokół rejestracji GARP VLAN (GVRP)

Mechanizmy związane z bezpieczeństwem sieci:



- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przetąacznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
- Obsługa HTTPS, SSH, SSL
- Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przetąacznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)

Mechanizmy związane z zapewnieniem jakości usług w sieci:

- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round Robin dla obsługi kolejek
- Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

Obsługa standardów komunikacyjnych:

IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet

Obsługa protokołu NTP

Funkcje DHCP server, DHCP relay

Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping

Blokowanie Head of Line (HOL)

Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)

Zapobieganie atakom DoS

Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6

Routing dynamiczny RIP v2

Zarządzanie

- Port konsoli



- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
- Obsługa protokołów SNMPv3, SSHv2, https, syslog
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Obsługa protokołu LLDP i LLDP-MED

Obsługa funkcji Plug & Play

Przycisk reset

Zasilanie 230V AC

Wysokość maksymalnie 1U, montowany w szafie typu RAC 19"

5.10. Firewall - klaster – szt. 1 – wymagania minimalne

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
 - 8 portami Gigabit Ethernet RJ-45.
 - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 120 GB.
5. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 64 B.



4. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
6. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy StatefullInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wystanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

14. 2. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
15. 3. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
16. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
18. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
19. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
20. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - Nuage Networks VSP.
 - OpenStack.
 - VMwarevCenter (ESXi).
 - VMware NSX.
 - VMwareNSX.Nutanix.



- VMware NSX.IBM Cloud.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/CounterMode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20 oraz 21.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-sharedkey, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPsec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPsecsite-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPsec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equalcostmulti-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (BidirectionalForwardingDetection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).
3. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu.
4. Rozwiązanie powinno wspierać funkcję Forward Error Correction na tunelach IPsec.
5. Funkcja monitorowania łączy w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.



4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW



1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
9. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
10. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
11. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo.
12. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie



1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandboxcloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

5.11. Centralny system logów – szt. 1 – wymagania minimalne

Wymagania Ogólne

W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 1TB

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
 - a. Listę najczęściej wykrywanych ataków.
 - b. Listę najbardziej aktywnych użytkowników.
 - c. Listę najczęściej wykorzystywanych aplikacji.
 - d. Listę najczęściej odwiedzanych stron www.
 - e. Listę krajów, do których nawiązywane są połączenia.
 - f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przysyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przestania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - Malware.
 - Aplikacje sieciowe.
 - Email.
 - IPS.
 - Traffic.
 - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
 - a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

5.12. Centralny UPS – szt. 1 – wymagania minimalne

Lp.	Opis wymagań techniczno-funkcjonalnych	Wartość minimalna
1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
2.	Budowa	Beztransformatorowa, prostownik IGBT. UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i Bypassu.
3.	Moc znamionowa	30 kVA / 30kW
4.	Wyjściowy współczynnik mocy (PF)	1,0
5.	Współczynnik mocy wejściowej 0.99.	0,99
6.	Napięcie wejściowe trójfazowe	400 VAC 3F + N



7.	Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie	172 – 287 Vac (L-N)
8.	Zakres częstotliwości wejściowej	Wymagana 40-70 Hz
9.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 96%
10.	Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza	Wymagany
11.	Możliwość rozbudowy mocy w okresie eksploatacji	Do minimum 8 sztuk w układzie pracy równoległej
12.	Montażu modułu pracy równoległej w oferowanej jednostce	Wymagane – pozwala na dołączenie kolejnej jednostki.
13.	Napięcie wyjściowe trójfazowe	400 VAC 3F + N
14.	Częstotliwość wyjściowa	50/60Hz (programowalna)
15.	Zintegrowane bezprzerwowe przetącniki obejściowe (by-pass)	Statyczny przetącnik (SCR) oraz ręczny rozłącznik serwisowy
16.	Zewnętrzny bezprzerwowy Bypass serwisowy	Wymagany Bypass bezprzerwowy w postaci jednego przetącnika, z informacją o położeniu dla zabezpieczenia falownika UPS przed uszkodzeniem w przypadku nieprawidłowego użycia.
17.	Wejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przetącnika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przetączeniem	Wymagane
18.	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem.	Wymagane, wraz z funkcją restingu baterii
19.	Możliwość regulacji prądu ładowania baterii z poziomu panelu LCD w UPS-ie.	Wymagane – podać maksymalną wartość prądu ładowania baterii
20.	Czas podtrzymania	6 minut przy obciążeniu 30kW
21.	Minimalna pojemność zainstalowanych akumulatorów liczona jako: Ilość akumulatorów * pojemność pojedynczego akumulatora * napięcie pojedynczego akumulatora [V*Ah]	8 640 Ah*V
22.	Moduł baterii	Baterie muszą być umieszczone w obudowie UPS. Należy stosować baterie szczelne AGM VRLA o żywotności 10-12 lat. Każdy łańcuch baterii zabezpieczony niezależnym rozłącznikiem bezpiecznikowym.
23.	Autonomia pracy zasilacza UPS przy pracy z baterii podawana w minutach na panelu LCD zasilacza	Wymagane
24.	W przypadku uszkodzenia pojedynczych akumulatorów w stosie, wymagana poprawna praca urządzenia ze zmniejszonym łańcuchem baterii	Wymagane, poprzez konfigurację, zmianę długości łańcucha baterii 30-40 sztuk
25.	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%
26.	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
27.	Stabilność częstotliwości wyjściowej:	bez synchronizacji: ± 0,05 Hz
28.	Współczynnik szczytu	3:1



29.	Minimalne przeciążenie falownika w trybie pracy normalnej	115% przez 60 minut 130% przez 10 minut 150% przez 1 minutę >150% - 0,2 sek
30.	Panel sterujący z wyświetlaczem dotykowym oraz sygnalizacją diodową i akustyczną	Wymagane
31.	Złącze interfejsów	SNMP, Dry Contact In/OUT, Modbus RTU, RS485
32.	Karta sieciowa SNMP wbudowana w UPS.	Wymagane
33.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane – zestyk NO oraz NC. UPS zintegrowany z systemem ppoż budynku.
34.	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
35.	Dedykowane oprogramowanie do wysyłania SMS	Wymagane
36.	Poziom hałasu w odległości 1m	< 50 dBA
37.	Rejestr zdarzeń	Dziennik zdarzeń w UPS-ie + komunikaty serwisowe
38.	Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
39.	Monitorowanie stanu baterii i czasu autonomii	Stan baterii + dostępna autonomia mierzona w czasie rzeczywistym
40.	UPS wyposażony w dotykowy, kolorowy wyświetlacz zabezpieczony hasłem przed ingerencją osób postronnych	Wymagane
41.	UPS wyposażony w programowany tryb pracy ECO mode o podwyższonej sprawności z możliwością zaprogramowania dni tygodnia oraz godzin w jakich UPS przechodzi automatycznie w tryb oszczędnej pracy o podwyższonej sprawności.	Wymagane
42.	UPS wyposażony w funkcję automatycznego czyszczenia z możliwością zaplanowania okresowego samoczynnego załączenia się tej funkcji.	Wymagane
43.	UPS wyposażony w zdalny wyłącznik REPO	Wymagane – dostawa po stronie dostawcy UPS.
44.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane zarówno dla zasilacza UPS jak i baterii
45.	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane
46.	Certyfikat ISO 9001 i 14001 dystrybutora i producenta sprzętu. Dopuszcza się certyfikaty równoważne potwierdzające posiadanie systemu zarządzania jakością i systemu zarządzania środowiskowego	Wymagane
47.	Rozłączniki manewrowe	Zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPSa. Wymaga się co najmniej czterech rozłączników zamontowanych na UPS: zasilanie prostownika, zasilanie bypass,



		bypass serwisowy, rozłącznik wyjściowy z UPS.
48.	Podłączenie zasilania i odbiorów	Podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego.
49.	UPS powinien posiadać funkcję umożliwiającą samo dociążenie bez podłączania dodatkowych odbiorników w celu przetestowania podzespołów pod pełnym obciążeniem w trakcie każdej wizyty serwisu.	Wymagane
50.	Zasilacz wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji	Wymagane
51.	Wymiary UPS nie większe niż (S x G x W)	300 x 850 x 1250 mm (+/-5%)
52.	Instrukcja w języku polskim	Wymagane

5.13. Instalacja i konfiguracja (Platforma sprzętowa) – wymagania minimalne

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.		
1.	Usługi	Celem prac jest przygotowanie środowiska teleinformatycznego – platformy sprzętowej, na potrzeby realizacji elementów Zintegrowanego Systemu Informatycznego i cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Część sprzętowa powinna zostać oparta na rozbudowie systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym: - Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązanie dla sytuacji kryzysowych wdrożenia. - Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: - koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu



		z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych. ii. schematy połączeń iii. mechanizmy działania głównych elementów sprzętowych: • Firewall/UTM • klaster wirtualizacyjny • system backupu i archiwizacji danych • system serwerowy • system macierzowy iv. iii. mechanizmy działania głównych elementów programowych: • Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR) • Oprogramowanie do zarządzania infrastrukturą IT. v. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności vi. sposób odbioru uzgodniony z Zamawiającym vii. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu viii. opis przypadków, w których projekt dopuszcza niedziałanie systemu ix. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.
2.	Montaż i fizyczne uruchomienie systemu	Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie: 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modułarnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).



		9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem: - Stworzenia połączeń sieci LAN pomiędzy przełącznikami. - Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. - Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. - Połączenia muszą wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	Instalacja/aktualizacja i konfiguracja oprogramowania	- Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. - Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. - Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). - Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych. - Instalacja i konfiguracja oprogramowania do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR) - Instalacja i konfiguracja oprogramowanie do zarządzania infrastrukturą IT.
4.	Konfiguracja przełączników/sieci LAN:	Re/Konfiguracja przełączników w zakresie: - Przeprowadzenie audytu obecnej topologii oraz konfiguracji. - Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). - Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy) - Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall. - Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. - Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; - Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). - Testowanie obsługi ruchu sieciowego. - Testowanie skuteczności zabezpieczeń.
5.	Konfiguracja elementów bezpieczeństwa sieciowego.	Konfiguracja/Modernizacja konfiguracji UTM dla nowych urządzeń w zakresie. - Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. - Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.



		3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Przygotowanie projektu włączenia dostarczonego urządzenia do sieci LAN urzędu – stworzenie klaster HA. 5. Konfiguracja dostarczonych systemów Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; e. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN. 11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekazuje Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zaporę ogniową klasy Stateful Inspection
--	--	---



		b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma 13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi. 14. Konfiguracja logowania i raportowania.
6.	Serwery, dyskowa macierz	Zamawiający wymaga wykorzystania istniejących serwerów i macierzy (klaster niezawodnościowy i wydajnościowy) na potrzeby instalacji i konfiguracji dostarczonego ZSI. Ilość i wielkość (udziałów dyskowych) maszyn wirtualnych dla serwerów zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeńiowej.
7.	Schemat systemu logiczny	Logiczny schemat rozbudowywanego systemu – stan docelowy. Serwery wirtualne System wirtualizacji – chmura prywatna Serwer #1 Wirtualizacyjny Istniejący Serwer #2 Wirtualizacyjny Istniejący Macierz Dyskowa Istniejąca NAS-Backup Istniejący Przełącznik sieci LAN CORE#1 Do zakupu Przełącznik sieci LAN CORE#2 Do zakupu Przełącznik sieci LAN IDF#1 Istniejący Przełącznik sieci LAN IDF#1 Istniejący Komputery Do zakupu UPS – do zakupu AGREGAT – do zakupu Centralny system logów Do zakupu Klaster firewall Firewall #1 Do zakupu Firewall #2 Do zakupu Laptopy Do zakupu INTERNET
8.	UPS	W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanych urządzeń UPS do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy.
9.	Migracja danych	Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów.



		Dane (systemy dziedziczne) muszą zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzicznych.
10.	Serwer SMTP	Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux. Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z: • Urządzeń sieciowych • Serwerów • Macierzy dyskowej • Systemu zarządzania kopiami zapasowymi • Systemu wirtualizacji serwerów • Aplikacji Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.
11.	Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.	1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przetłaczników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy. 2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego). 3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie. 4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
12.	Aktualizacja środowiska wirtualizacyjnego.	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta. 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.



		6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) $n-(n-1)$ ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) $n-(n-1)$ ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 11. Konfiguracja klastra wysokiej dostępności: a. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika. b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn. c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 12. Weryfikacja działania klastra wysokiej dostępności. 13. Migracja istniejącej infrastruktury do środowiska wirtualnego. 14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
13.	Rekonfiguracja systemu zarządzania kopiami zapasowymi.	1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na serwerze backupu (wgranie licencji). 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:



		a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej: a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. Zapetnienia mail-slotu 8. Uruchomienie testowych zadań backupu 9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email 10. Uruchomienie testowych zadań odtworzenia danych 11. Miejscem przechowywania kopii zapasowych jest: a. serwer backupu. b. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym 12. Do serwera backupu należy podłączyć istniejąca macierz, oraz system NAS. System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.
14.	Oprogramowanie do monitorowania i	1. Proces wdrożenia systemu określony powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne



	analizy cyberbezpieczeństwa	wdrożenie rozwiązania w okresie 3 miesięcy. 2. Proces wdrożeniowy podzielony zostanie na obszary: - Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji). - Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM. - Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR. 3. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno: - Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac). - Uruchomienie systemu w infrastrukturze zamawiającego, w tym: - konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu, - przygotowanie przez Zamawiającego połączenia zdalnego, - instalację lub import maszyny wirtualnej typu „software appliance”, - aktywację licencji, - wstępną konfigurację, - import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN). - Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym: - przekierowanie logów opisujących transmisję sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu, - uruchomienie reguł wykrywania. - Prace audytowe, w tym: - pasywną analizę transmisji sieciowej: - o ruch z/do serwerów webowych i aplikacyjnych, - o ruch z/do serwerów baz danych, - o ruch z/do serwerów pocztowych, - o ruch z/do kontrolerów domenowych, - o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP), - o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji. - konsultacje w ramach otrzymanych wyników, - zebranie danych audytowych wymaganych do sporządzenia raportu. - Analizę podatności, w zakresie: - integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source,
--	---	--



		• przygotowanie reguł priorytetów i importu krytycznych podatności. f. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przetwarzania zabezpieczeń organizacji. Raport powinien zawierać: • zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia, • potencjalne wektory ataków dla wykrytych zagrożeń, • wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków, • rekomendacja zabezpieczeń, • zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przetwarzania zabezpieczeń. 4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno: a. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują: • zapory sieciowe w punktach styku z siecią Internet (Firewall brzegowy), • sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam), • centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR), • kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym, • systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA), • system SIEM, • źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji, b. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą. c. Podłączenie reguł detekcji. d. Podłączenie i konfiguracja mechanizmów UEBA: • integracja z Active Directory, • adaptacja profili użytkowników UBA, • adaptacja profili hostów EBA, • import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia. 5. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać: a. Import gotowych scenariuszy obsługi. b. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi.
--	--	---



		c. Konfigurację mechanizmów powiadamiania. 6. Usługa konsultacji powdrożeniowej, świadczona przez dedykowanego inżyniera w ramach okresu wsparcia musi w szczególności uwzględniać: - przygotowanie i modyfikację formularzy raportów; - tworzenie i edycję parserów; - przygotowywanie nowych reguł bezpieczeństwa; - modyfikację dostępnych reguł i ich dostrojenie; - wsparcie w procesie aktualizacji systemu; - tworzenie i edycję nowych scenariuszy reakcji; - tworzenie i dostosowanie dashboardów danych. 7. 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. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 5 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/systemów. Szkolenia mogą odbyć się w formie zdalnej.
15.	Oprogramowanie do zarządzania infrastrukturą IT.	System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.
16.	Testowanie i modyfikacja parametrów infrastruktury sieciowej.	- Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. - Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. - Testowanie mechanizmów replikacji danych. - Testowanie dostępu publicznego do zasobów. - Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu - Testowanie autoryzowanego dostępu do wewnętrznych zasobów. - Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
17.	Asysty stanowiskowe	Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć

		w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia. Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.
18.	Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30. W tym czasie przedstawiciel Wykonawcy: • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. • dokona prezentacji działania systemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) wirtualizacji d) systemu backupu e) zastosowanych rozwiązań aplikacyjnych Wykonawca zapewni również wsparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
19.	Opracowanie dokumentacji powykonawczej	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.



		5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.
20.	Opieka serwisowa	Zamawiający wymaga świadczenia opieki serwisowej przez okres wskazany w pkt. 4.1 z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.

6. Szczegółowy opis pozycji – część 2.

6.1. Agregat – szt. 1 – wymagania minimalne

1. Moc wg PN-ISO 8528 (+/-5%): PRP min. 60 kVA / 48 kW LPT (SB) min. 70 kVA / 56 kW 2. Napięcie nominalne: 3x 400 VAC / 50 Hz 3. Prędkość obrotowa: 1500 obr/min 4. Klasa regulacji (ISO 8528-5): G2 lub równoważne 5. Regulator silnika: elektroniczny 6. Agregat obudowany i wyciszony o głośności nie większej niż 70 dB z 7 metrów 7. Obudowa wykonana z materiałów odpornych na korozję 8. Maksymalne wymiary obudowy nie większe niż 2500 x 1000 x 1700 mm (D x S x W) 9. Zbiornik paliwa – min. 100L. 10. Drzwi serwisowe po obu stronach obudowy + 1 drzwi do panelu sterowania 11. Dostęp do chłodnicy poprzez przy pomocy zdejmowanego panelu 12. Spawana, stalowa rama agregatu wyposażona w zbiornik paliwa na 12 godzin pracy z pełnym obciążeniem 100% PRP 13. Zamki i okucia obudowy wykonane ze stali nierdzewnej 14. Wskaźnik poziomu paliwa 15. Wlew paliwa na obudowie, zabezpieczony na klucz 16. Możliwość dotankowania podczas pracy agregatu 17. Agregat wyposażony w układ podgrzewania cieczy chłodzącej umożliwiający start zespołu w niskich temperaturach. Układ podgrzewania musi posiadać termostat umożliwiający regulację zadanej temperatury 18. Tłumiki wibroizolacyjne pomiędzy ramą, a zespołem silnikiem i prądnicą 19. Tłumik wydechu 20. Agregat z bieżącej produkcji, nowy 21. Pompa do spuszczenia oleju silnikowego 22. Spalanie silnika Diesla nieprzekraczające 17 l/h przy 100% obciążenia PRP 23. Zalecane przez producenta silnika przeglądy nie częściej niż co 500 motogodzin. 24. Konstrukcja prądnicy: synchroniczna, samowzbudna, samoregulująca, bez-szczotkowa, jednotożyskowa 25. Sprawność prądnicy przy 100% PRP min 88,5 % 26. Panelu automatyki wyposażony w sterownik mikroprocesorowy z cyfrowym wyświetlacz LCD oraz diody sygnalizujące tryb pracy agregatu oraz sieci 27. Panel automatyki posiadający minimum 7 wejść binarnych, 7 wyjść binarnych, 3 wejścia analogowe 28. Panel sterowania przygotowany do pracy w trybach: ręcznym, automatycznym i testowym. 29. Możliwość zastosowania komunikacji zdalnej SNMP oraz MODBUS RTU 30. Wejście do podania sygnału startu i stopu z zewnętrznego układu SZR 31. Możliwość sterowania zewnętrznym układem SZR 32. Menu sterownika w języku polskim 33. Historia zdarzeń sterownika min. 100 wpisów 34. Agregat wyposażony w wyłącznik 3-biegunowy 35. Minimalny okres gwarancji – 5 lat	36. Instalacja i uruchomienie urządzenia Zamawiający wymaga przeprowadzenia prac instalacyjnych i montażowych urządzenia, włączenia go do sieci energetycznej Urzędu oraz przeprowadzenia pierwszego uruchomienia. Wykonawca jest zobowiązany uwzględnić w ofercie wszystkie koszty z tym związane.
--	--



7. Szczegółowy opis pozycji – część 3.

7.1. Zestaw komputerowy z oprogramowaniem – szt. 20 – wymagania minimalne

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Komputer	Komputer fabrycznie wbudowany w obudowę monitora. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
2.	Obudowa	Obudowa typu All-in-One z możliwością zabezpieczenia fizycznego przez metalową linkę typu Kensington Lock oraz umożliwiającą beznarzędziową wymianę pamięci RAM. Wypozazona w listwę montażową w standardzie VESA 100x100. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym
3.	Podstawa	Podstawa umożliwiająca regulację jednostki w zakresie co najmniej: - pochylenie przód tył od -5 do 20 stopni - swivel w zakresie 45 stopni w każdą stronę - pivot w zakresie 90 stopni - regulację wysokości w do 110mm
4.	Chipset	Dostosowany do zaoferowanego procesora
5.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 3 złącza M.2 z czego 2 dedykowane dla dysku SSD PCIe. Płyta główna wyposażona w min. 2 sloty pamięci RAM DDR5.
6.	Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark - Multithread Rating wynik co najmniej 25800 pkt. według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Wynik nie starszy niż 90 dni od daty złożenia oferty. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
7.	Pamięć operacyjna	Min. 16GB RAM, Możliwość rozbudowy do min. 64GB Jeden slot pozostawiony wolny
8.	Dysk twardy	Min 512GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku OPAL, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość instalacji drugiego dysku SSD M.2
9.	Karta graficzna	Zintegrowana karta graficzna z procesorem.
10.	Matryca	Min. 23,8" IPS o rozdzielczości min. FHD 1920x1080 Jasność typowa min. 250 cd/m ² Kontrast typowy min. 1300:1 Typowy czas reakcji matrycy maksymalnie 14ms Odświeżanie min. 60Hz Gamut min. 99% sRGB Sprzętowa funkcja redukująca emisję światła niebieskiego Kąty widzenia poziomo/pionowo min. 178/178 stopni
11.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane dwa głośniki o mocy min. 3W każdy Wbudowane dwa mikrofony. Kamera min. 5MP zintegrowana z obudową komputera, z mechaniczną zastoną obiektywu, funkcją logowania za pomocą rozpoznawania twarzy oraz możliwością regulacji pochylenia w zakresie od -20 do 20 stopni.



12.	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 Wbudowana karta sieci bezprzewodowej, pracująca w standardzie AX Bluetooth min. 5.1
13.	Porty/złącza	Z tyłu obudowy: - 1 x USB 3.2 typu C Generacji 2 - 3 x USB 3.2 typu A Generacji 1 - 1 x HDMI combo - 1x DisplayPort 1.4 - 1x RJ-45 Z boku obudowy: - 3x USB 3.2 typu A Generacji 2 - 1x złącze audio combo Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
14.	Klawiatura/mysz	Przewodowa USB: klawiatura w układzie US + mysz z rolką
15.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 180W oraz sprawności na poziomie min. 90%.
16.	Ergonomia	Głośność jednostki w konfiguracji oferowanej lub wyższej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w trybie jałowym (IDLE) ma wynosić maksymalnie 22dB
17.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1.Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2.Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego 3.Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4.Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI. 5.Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7.Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8.Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9.Wbudowany system pomocy w języku polskim. 10.Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11.Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12.Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13.Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.



	14.Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15.Możliwość dotłączenia systemu do usługi katalogowej on-premise lub w chmurze. 16.Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17.Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18.Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19.Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20.Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21.Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22.Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23.Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24.Wbudowany mechanizm wirtualizacji typu hypervisor." 25.Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26.Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27.Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28.Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29.Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30.Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31.Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32.Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33.Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34.Możliwość tworzenia wirtualnych kart inteligentnych. 35.Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36.Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37.Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38.Mechanizmy logowania w oparciu o:
--	--



		a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
18.	BIOS	Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym, - numerze inwentarzowym (AssetTag), - MAC Adres karty sieciowej, - wersji BIOS, - dacie produkcji BIOS - zainstalowanym procesorze, - zainstalowanej pamięci RAM, - urządzeniach podłączonych do portów M.2 Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB - wyłączenia karty sieciowej - wyłączenia karty audio - wyłączenia funkcji Wake on LAN - wyłączenia wirtualizacji - wyłączenia modułu TPM - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, dysku twardego - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania sekwencji bootowania, z uwzględnieniem PXE, zewnętrznych nośników, dysku twardego - załadowania optymalnych ustawień Bios bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
19.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający wykonanie diagnostyki następujących podzespołów:



		• test pamięci RAM • test dysku twardego • test portów USB • test płyty głównej • test procesora Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregośkolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikację testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja, data wydania, producent • Procesor : Nazwa, taktowanie, liczba rdzeni, liczba wątków, pamięć cache L1, L2, L3 • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny, taktowanie • Dysk twarde: model, numer seryjny, wersja firmware, pojemność, temperatura pracy, producent • System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
20.	Certyfikaty i standardy	Dla producenta sprzętu - ISO 9001 lub równoważny - ISO 14001 lub równoważny - ISO 50001 lub równoważny Dla komputera: - Deklaracja zgodności CE - TUV Rheinland Low Blue Light - TUV Rheinland Flicker Free - MIL-STD-810H
21.	Bezpieczeństwo	- Złącze typu Kensington Lock - Moduł TPM 2.0 z certyfikacją TCG - Czujnik otwarcia obudowy
22.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
23.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie.
24.	Gwarancja i wsparcie techniczne producenta	Świadczona w miejscu użytkowania sprzętu (on-site). Minimalny okres gwarancji – 5 lat. Firma serwisująca posiadająca certyfikat systemu zarządzania jakością na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:



		- fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera. W przypadku awarii dysku, dysk twardy pozostaje u Zamawiającego.
25.	Pakiet biurowy	Pakiet biurowy spełniający następujące wymagania techniczne: Licencja wieczysta Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; • oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleczeń, język skryptowy); • do aplikacji musi być dostępna pełna dokumentacja w języku polskim; Pakiet zintegrowanych aplikacji biurowych musi zawierać: • edytor tekstów, • arkusz kalkulacyjny, • narzędzie do przygotowywania i prowadzenia prezentacji, • narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami), 1. Edytor tekstów musi umożliwiać: • edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, • wstawianie oraz formatowanie tabel, • wstawianie oraz formatowanie obiektów graficznych, • wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), • automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, • automatyczne tworzenie spisów treści, • formatowanie nagłówków i stopek stron, • śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • określenie układu strony (pionowa/pozioma), • wydruk dokumentów, • wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, • wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako

		środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, 2. Arkusz kalkulacyjny musi umożliwiać: • tworzenie raportów tabelarycznych, • tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, • tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, • tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, Webservice), • obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, • tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, • wyszukiwanie i zamianę danych, • wykonywanie analiz danych przy użyciu formatowania warunkowego, • nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, • nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleczeń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; 3. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016;
--	--	---



		4. Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonego z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
--	--	--

7.2. Laptopy – szt. 12 – wymagania minimalne

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer przenośny.
2.	Procesor	Procesor ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core Ultra 5 125U na podstawie wyników Passmark CPU Mark z dnia XYZ opublikowanych na stronie http://www.cpubenchmark.net/ . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
3.	Pamięć operacyjna RAM	Min. 16GB DDR5 pracującej w trybie dual channel Możliwość rozbudowy pamięci do min. 64GB
4.	Parametry pamięci masowej	M.2 512 GB SSD PCIe 4.0 x4 NVMe Przygotowana, wolna zatoka do rozbudowy komputera o dodatkowy dysk SSD.
5.	Karta graficzna	Procesor dedykowany do pracy w komputerach przenośnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark - Multithread Rating wynik co najmniej 17750 pkt. według wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php Wynik nie starszy niż 90 dni od daty złożenia oferty. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
6.	Wposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo 2x2W, port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zastoną obiektywu oraz obsługująca logowanie za pomocą danych biometrycznych z obsługą między Windows Hello, dwa mikrofony z funkcją wygłuszania niechcianych odgłosów tła, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszenia głośników oraz mikrofonu (mute).
7.	Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H.
8.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny urządzenia.



9.	Bezpieczeństwo	Moduł fTPM 2.0 lub dTPM 2.0 Slot typu Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington. Dysk systemowy zawierający partycję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
11.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - typie procesora - ilości pamięci RAM Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła administratora - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość włączenia/wyłączenia bootowania z USB oraz PXE - Możliwość Wyłączania/Włączania: karty sieciowej, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, USB
12.	Bezpieczeństwo – System Diagnostyczny	Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednocześnie przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych: 1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: - pamięci ram, - procesora, - pamięci masowej, - płyty głównej. 2. Identyfikację jednostki i jej komponentów w następującym zakresie: - urządzenie (producent, model, numer seryjny), - bios (producent, wersja oraz data wydania), - procesor (nazwa, taktowanie, ilości pamięci cache), - pamięć ram (ilość zainstalowanej pamięci ram, producent), - dysk twardy (producent, model, numer seryjny, pojemność).
13.	Ekran	Matowy, matryca IPS min. 14" max. 16" 16:10 z podświetleniem w technologii LED, rozdzielczość min. WUXGA 1920x1200, jasność min. 300 nits, kąt otwarcia pokrywy ekranu min. 180 stopni.
14.	Interfejsy / Komunikacja	- 2x USB 3.2 typu A - 1x ThunderBolt 4 - 1x USB 3.2 typu C



		- 1x HDMI - 1x złącze audio combo - 1x RJ-45 - 1x czytnik kart SD wbudowany lub w formie przejściówki USB Nie dopuszcza się osiągnięcia wymaganych portów USB poprzez zastosowanie przejściówek.
15.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie min. Wi-Fi 6E 11ax Bluetooth min. 5.3
16.	Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, wyposażona w min. 2 tryby podświetlania przycisków (włączone, wyłączone)
17.	Czytnik linii papilarnych	Czytnik linii papilarnych wbudowany w klawiaturę lub przycisk zasilania. Przycisk zasilania znajdujący się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia. Nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury.
18.	Akumulator	O pojemności min. 45Wh
19.	Zasilacz	Zasilacz zewnętrzny USB-C min. 65W
20.	Certyfikaty, oświadczenia i standardy	Dla producenta sprzętu należy dostarczyć certyfikat: - ISO 9001 lub równoważny - ISO 14001 lub równoważny - ISO 50001 lub równoważny Dla komputera: - Deklaracja zgodności CE
21.	Waga	Waga startowa urządzenia nie większa niż 1.75kg według karty katalogowej producenta
22.	System operacyjny	System operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przetaczanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.



	13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zaporą internetową (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
--	---



		37.Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38.Mechanizmy logowania w oparciu o: - Logín i hasło, - Karty inteligentne i certyfikaty (smartcard), - Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), - Certyfikat/Klucz i PIN - Certyfikat/Klucz i uwierzytelnienie biometryczne 39.Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40.Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41.Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42.Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43.Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
23.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
24.	Gwarancja i wsparcie techniczne producenta	Gwarancji producenta sprzętu, świadczonej w miejscu użytkowania (on-site). Minimalny okres gwarancji – 5 lat. Bezpłatna infolinia w języku polskim, funkcjonująca minimum w godzinach 9:00 – 16:00 oraz obsługująca zgłoszenia serwisowe i oferująca wsparcie techniczne w zakresie co najmniej: - wsparcia technicznego dla zakupionego sprzętu, - weryfikacji konfiguracji fabrycznej zakupionego sprzętu, - weryfikacji statusu gwarancji zakupionego sprzętu. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej: - fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach. Diagnostyka sprzętowa dostępna na stronie internetowej producenta
25.	Pakiet biurowy	Pakiet biurowy spełniający następujące wymagania techniczne: • Licencja wieczysta • Wymagania odnośnie interfejsu użytkownika: • pełna polska wersja językowa interfejsu użytkownika, • prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; • oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: • posiada kompletny i publicznie dostępny opis formatu, • w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); • do aplikacji musi być dostępna pełna dokumentacja w języku polskim; Pakiet zintegrowanych aplikacji biurowych musi zawierać:



- edytor tekstów,
- arkusz kalkulacyjny,
- narzędzie do przygotowywania i prowadzenia prezentacji,
- narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami),

1. Edytor tekstów musi umożliwiać:

- edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
- wstawianie oraz formatowanie tabel,
- wstawianie oraz formatowanie obiektów graficznych,
- wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
- automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
- automatyczne tworzenie spisów treści,
- formatowanie nagłówków i stopek stron,
- śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
- nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
- określenie układu strony (pionowa/pozioma),
- wydruk dokumentów,
- wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
- zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
- wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,

2. Arkusz kalkulacyjny musi umożliwiać:

- tworzenie raportów tabelarycznych,
- tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
- tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
- tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, Webservice),
- obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,
- tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
- wyszukiwanie i zamianę danych,
- wykonywanie analiz danych przy użyciu formatowania warunkowego,
- nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,

		• nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, • formatowanie czasu, daty i wartości finansowych z polskim formatem, • zapis wielu arkuszy kalkulacyjnych w jednym pliku, • zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, • zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; 3. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: • przygotowywanie prezentacji multimedialnych, • prezentowanie przy użyciu projektora multimedialnego, • drukowanie w formacie umożliwiającym robienie notatek, • zapisanie jako prezentacja tylko do odczytu, • nagrywanie narracji i dołączanie jej do prezentacji, • opatrywanie slajdów notatkami dla prezentera, • umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, • umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, • odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, • prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, • pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016; 4. Narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać: • pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • przechowywanie wiadomości na serwerze lub w lokalnym pliku stworzonym z zastosowaniem efektywnej kompresji danych, • filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, • tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, • automatyczne grupowanie poczty o tym samym tytule, • tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
--	--	--

Zatwierdzam:


mgr Bogusław Kręcisz