

## **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Opracowany dokument określa minimalne wymagania dla dostaw i usług stanowiących przedmiot niniejszego postępowania. Wymagania określone w niniejszym dokumencie mają na celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawy i usługi teleinformatyczne, których podstawowym celem jest podniesienie poziomu cyberbezpieczeństwa w Urzędzie Gminy w Kamieniu. Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych oraz jakościowych, a także wskazuje technologie, które muszą być wykorzystane, aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.

### **Wymagania ogólne dla urządzeń i oprogramowania**

1. Dostarczony sprzęt i rozwiązania teleinformatyczne muszą być fabrycznie nowe (rok produkcji 2024/2025). Sprzęt nie może być używany, odnawiany, eksponowany na wystawach, targach lub prezentacjach, musi być wolny od wad, uszkodzeń oraz musi być wolny od obciążeń prawami osób trzecich.
2. Oferowany sprzęt musi być objęty gwarancją producenta lub gwarancją partnera serwisowego producenta i musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej.
3. Wszystkie urządzenia powinny być zgodne z normami UE oraz powinny posiadać wymaganą certyfikację oraz oznaczenie CE.
4. Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów lub akcesoriów.
5. Dostarczone oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności, wymagane przez producenta oprogramowania w zależności od dostarczanej wersji oprogramowania.
6. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy oferowanych zestawów oraz podzespoły były certyfikowane przez producenta urządzenia lub znajdowały się na liście kompatybilności oferowanego urządzenia.

### **Warunki dotyczące realizacji dostaw i odbiorów:**

1. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
2. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, m.in. rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
3. Wykonawca, co najmniej na 2 dni przed dniem planowanej dostawy sprzętu, skontaktuje się z Zamawiającym w celu potwierdzenia dokładnej daty dostawy.
4. Adres dostawy: Urząd Gminy Kamień, Kamień 287, 36-053 Kamień.
5. Dostawa odbędzie się w dniu roboczym, od poniedziałku do piątku, w godzinach pracy Urzędu Gminy w Kamieniu, transportem zapewnionym przez Wykonawcę, na jego koszt i ryzyko wraz z wniesieniem do pomieszczenia wskazanego przez Zamawiającego.

6. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
7. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń oraz wszelką dokumentację dostarczoną przez producenta sprzętu.
8. W ramach procedury odbioru, Zamawiający zastrzega sobie prawo do przeprowadzenia weryfikacji oryginalności i legalności dostarczonego przez Wykonawcę oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny. W przypadku wykrycia, że dostarczony system operacyjny lub inne licencjonowane oprogramowanie jest nieoryginalne (nielegalne), nie jest nowe, było już używane lub było już wcześniej aktywowane, Zamawiający w takiej sytuacji odmówi przyjęcia licencji oprogramowania i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

**Warunki dotyczące realizacji usług:**

Realizacja usług opisanych w niniejszym dokumencie musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz przez osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

Architektura projektowanego i uruchomionego rozwiązania informatycznego, o którym mowa w niniejszym dokumencie powinna spełniać wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych. Zgodnie z zapisami §20 ust. 2 (KRI) system powinien spełniać wymagania w zakresie:

1. minimalizacji ryzyka utraty informacji w wyniku awarii,
2. zapewnienia bezpieczeństwa przechowywanych plików systemowych oraz innych, zapewnienia możliwości regularnej aktualizacji oprogramowania (nowy system będzie posiadał wsparcie techniczne producenta w okresie eksploatacji).

**Warunki dotyczące udzielenia gwarancji:**

1. Zamawiający wymaga dostarczenia rozwiązań teleinformatycznych opisanych z niniejszym dokumencie z gwarancją podstawową na okres nie krótszy niż 2 lata (24 miesiące).
2. Oferent ma możliwość zaoferowania serwerów, macierzy dyskowej oraz serwerów NAS z gwarancją rozszerzoną wydłużającą okres gwarancji podstawowej o dodatkowe 12, 24, 36 - jest to wymóg nieobowiązkowy (fakultatywny). Przy zaoferowaniu gwarancji rozszerzonej i po potwierdzeniu spełnienia tego kryterium (przez wpisanie w formularzu ofertowym przez Wykonawcę informacji o długości gwarancji rozszerzonej), Wykonawcy zostanie przyznana liczba punktów określona w kryteriach oceny ofert zgodnie z kryteriami określonymi w SWZ.
3. Zamawiający wymaga aby udzielona gwarancja podstawowa i/lub rozszerzona była gwarancją producenta realizowaną bezpośrednio przez producenta lub jego autoryzowany serwis.

**Pozostałe wymagania:**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania.

Wykonawca jest zobowiązany uwzględnić w cenie w ramach kosztów dodatkowych:

1. Koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) użytkownika przed ich zniszczeniem w trakcie wykonywania prac.
2. Koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego.
3. Koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac.
4. Koszty testów, prób, badań, odbiorów technicznych (jeśli będą wymagane).
5. Koszty opracowania dokumentacji użytkowej (powykonawczej) oferowanego rozwiązania, aby administratorzy/użytkownicy mogli w sposób właściwy z niego korzystać.
6. Koszty uporządkowania oraz przywrócenia obiektu po wykonanych pracach do stanu pierwotnego wraz z naprawą ewentualnych szkód użytkownikowi lub osobom trzecim.

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności min. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowanie minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega m. in. na:

1. Zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.
2. Redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych.
3. Zapewnienia bezpieczeństwa plików.
4. Dbłość o aktualizację oprogramowania.

Kolejnym istotnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń). Konieczność zapewnienia tej funkcjonalności wynika z:

1. §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej).
2. Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa.

Zamawiający wymaga dostawy sprzętu informatycznego oraz wykonania usług określonych w niniejszym dokumencie. Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu. Wdrożone rozwiązania powinny spełniać wymagania przywołanych aktów prawnych oraz standardów rynkowych.

## Spis treści

Obszar organizacyjny.....	4
Sporządzenie procedur i instrukcji SZBI, wdrożenie SZBI .....	4
Audyt SZBI, audyt zgodności KRI/uoKSC.....	4
Obszar techniczny.....	5
Zakup systemu SIEM/SOAR .....	5
Zakup serwerów do pracy w klastrze wysokiej dostępności HA (High Availability Cluster).....	28
Zakup licencji na serwerowy system operacyjny .....	33
Zakup licencji dostępowych CAL Device serwerowego systemu operacyjnego .....	36
Zakup licencji dostępowych CAL User serwerowego systemu operacyjnego .....	36
Zakup macierzy pamięci masowej (macierzy danych).....	37
Zakup urządzenia klasy UTM .....	39
Zakup zarządzalnego przełącznika sieciowego .....	47
Zakup serwera NAS z dyskami - typ 1 .....	48
Zakup serwera NAS z dyskami - typ 2.....	49
Zakup oprogramowania do realizacji kopii zapasowych ze wsparciem w okresie realizacji projektu .....	51
Zakup dysków zewnętrznych USB w celu przechowywania odseparowanych od sieci kopii zapasowych....	59
Zakup zasilaczy awaryjnych UPS typu Rack .....	59
Zakup zasilaczy awaryjnych UPS do stanowisk komputerowych.....	61
Zakup utrzymania wsparcia technicznego wraz z subskrypcjami dla posiadanego UTM.....	61
Zakup utrzymania wsparcia technicznego wraz z subskrypcjami dla posiadanego systemu do zarządzania zasobami IT.....	62
Zakup usług konfiguracyjnych pozwalających wdrożyć nowe rozwiązania informatyczne .....	63

## Obszar organizacyjny

### Sporządzenie procedur i instrukcji SZBI, wdrożenie SZBI

ATRYBUT	WYMAGANIA MINIMALNE
Zakres działania	<p>Zamawiający wymaga, aby usługa opracowania dokumentacji oraz wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) została zrealizowana zgodnie ze standardem ISO/IEC 27001:2022.</p> <p>Celem usługi jest zwiększenie ochrony danych i informacji w organizacji na poziomie technicznym oraz organizacyjnym, zapewnienie zgodności z obowiązującymi przepisami prawnymi, poprawa ogólnego poziomu bezpieczeństwa informacji zgodnie z normami wyrażonymi w PN ISO/IEC 27001.</p>

### Audyt SZBI, audyt zgodności KRI/uoKSC

ATRYBUT	WYMAGANIA MINIMALNE
Zakres działania	Zadanie obejmuje przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach organizacyjnych będących uczestnikami projektu.

	Audyt musi zostać przeprowadzony w zakresie spełniającym wymagania określone w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem <a href="https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad">https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad</a>
Uprawnienia audytora	Audyt musi zostać przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

## Obszar techniczny

### Zakup systemu SIEM/SOAR

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy podać pełną nazwę handlową oferowanego rozwiązania, w tym producenta, model (symbol, wersję) oferowanego rozwiązania oraz podstawowe parametry rozwiązania jeśli są wymagane w formularzu ofertowym.
Ilość	1 zestaw
Funkcjonalności, cechy	<p>Zamawiający wymaga dostawy licencji na platformę zapewniającą przeciwdziałania cyberzagrożeniom, oferującą możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności.</p> <ol style="list-style-type: none"> <li>1. Przedmiotem zamówienia jest zakup systemu przeciwdziałającego cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.</li> <li>2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje co najmniej następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.</li> <li>3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.</li> <li>4. 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.</li> <li>5. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.</li> <li>6. 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.</li> <li>7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości</li> </ol>

	<p>lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.</p> <p>8. 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.</p> <p>9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.</p> <p>10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.</p> <p>11. 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.</p> <p>12. 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.</p> <p>13. 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.</p> <p>14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.</p> <p>15. 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.</p> <p>16. 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 zapelnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.</p> <p>17. 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</p>
--	--



	<p>repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.</p> <p>18. 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.</p> <p>19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.</p> <p>20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.</p> <p>21. 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.</p> <p>22. 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.</p> <p>23. 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.</p> <p>24. 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.</p> <p>25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.</p> <p>26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.</p> <p>27. 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.</p>
--	--

28. 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.
29. 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.
30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
32. 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.
33. 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.
34. 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/>).
35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).
36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi



	<p>publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).</p> <p>37. 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.</p> <p>38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.</p> <p>39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).</p> <p>40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.</p> <p>41. 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.</p> <p>42. 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.</p> <p>43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&amp;CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:</p> <ol style="list-style-type: none"> <li>a) id techniki,</li> <li>b) taktykę,</li> <li>c) platformy których dotyczy,</li> <li>d) potencjalne źródła,</li> <li>e) opis zagrożenia,</li> <li>f) mityzację,</li> <li>g) sposób detekcji,</li> <li>h) referencje.</li> </ol> <p>44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.</p> <p>45. 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</p>
--	--

	<p>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.: rozdzielanie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).</p> <p>46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:</p> <ol style="list-style-type: none"> <li>rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,</li> <li>rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,</li> <li>rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,</li> <li>rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.</li> </ol> <p>47. 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).</p> <p>48. 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.</p> <p>49. 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).</p> <p>50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.</p> <p>51. 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.</p> <p>52. 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:</p> <ol style="list-style-type: none"> <li>sparsowane pola oraz ich wartości,</li> <li>listy referencyjne,</li> <li>atrybuty użytkowników z Active Directory,</li> <li>atrybuty komputerów z Active Directory,</li> <li>bazę wskaźników kompromitacji (IOC),</li> <li>informacje z elektronicznej dokumentacji,</li> <li>anomalie w zachowaniu użytkowników (UBA),</li> <li>anomalie w zachowaniu zasobów (EBA),</li> <li>podatności na zasobach,</li> </ol>
--	--

	<p>j) wyniki analizy konfiguracji,</p> <p>k) techniki MITRE ATT&amp;CK®.</p> <p>53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:</p> <p>a) wykrycie dowolnej treści w logach,</p> <p>b) wykrycie zmiany jednego z kilku pól,</p> <p>c) wykrycie zaniku wiadomości,</p> <p>d) wykrycie nowej wartości pola w zadanym okresie czasu,</p> <p>e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,</p> <p>f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,</p> <p>g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,</p> <p>h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,</p> <p>i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,</p> <p>j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,</p> <p>k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,</p> <p>l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu,</p> <p>m) wykrycie skanowania portów.</p> <p>54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:</p> <p>a) wykrycie wystąpienia wartości pola na wybranej liście,</p> <p>b) wykrycie niewystępowania wartości pola na wybranej liście,</p> <p>c) wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony),</p> <p>d) wykrycie niewystąpienia pary wartości na wybranej liście</p> <p>e) (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).</p> <p>55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:</p> <p>a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,</p> <p>b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,</p> <p>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).</p> <p>d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),</p> <p>e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.</p>
--	---

	<p>56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,</li> <li>b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,</li> <li>c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.</li> </ul> <p>57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;</li> <li>b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;</li> <li>c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;</li> </ul> <p>58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,</li> <li>b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,</li> <li>c) wykrycie nieautoryzowanej usługi na serwerze,</li> <li>d) wykrycie nieautoryzowanego połączenia do usługi na serwerze,</li> <li>e) wykrycie nieautoryzowanego połączenia z serwera usług,</li> <li>f) wykrycie nieautoryzowanego połączenia do sieci Internet.</li> </ul> <p>59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,</li> <li>b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,</li> <li>c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,</li> <li>d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.</li> </ul> <p>60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,</li> <li>b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,</li> <li>c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,</li> <li>d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach.</li> </ul>
--	---

	<p>61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,</li> <li>b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,</li> <li>c) wykrycie zdarzeń o wysokim „severity” na zasobach posiadających krytyczne podatności,</li> <li>d) wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.</li> </ul> <p>62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:</p> <ul style="list-style-type: none"> <li>a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,</li> <li>b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.</li> </ul> <p>63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&amp;CK® muszą umożliwić:</p> <ul style="list-style-type: none"> <li>a) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,</li> <li>b) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,</li> <li>c) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.</li> </ul> <p>64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:</p> <ul style="list-style-type: none"> <li>a) wykrycie anomalii na koncie uprzywilejowanym użytkownika,</li> <li>b) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,</li> <li>c) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,</li> <li>d) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,</li> <li>e) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.</li> </ul> <p>65. 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:</p> <ul style="list-style-type: none"> <li>a) sparsowane pola oraz ich wartości,</li> <li>b) atrybuty użytkowników z Active Directory,</li> </ul>
--	---

	<p>c) atrybuty komputerów z Active Directory, d) informacje z elektronicznej dokumentacji.</p> <p>66. 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:</p> <p>a) adresie IP, b) koncie domenowym użytkownika, c) strefie bezpieczeństwa, d) zakresie adresów IP.</p> <p>67. 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 zmianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.</p> <p>68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.</p> <p>69. 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.</p> <p>a) wszystkie skorelowane zdarzenia, b) korespondencja pocztowa, c) załączniki z próbkami lub dowodami, d) wskaźniki kompromitacji (IoC), e) informacje pozyskane z innych systemów.</p> <p>70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.</p> <p>71. 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.</p> <p>72. 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:</p> <p>a) identyfikację celu i źródła zagrożenia, b) nazwę oraz adres IP źródła zagrożenia, c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja</p>
--	---



	<p>robocza,</p> <p>d) lokalizację z której pochodzi zagrożenie np.: Internet,</p> <p>e) strefę bezpieczeństwa z której pochodzi zagrożenie,</p> <p>f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,</p> <p>g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),</p> <p>h) nazwę oraz adres IP celu zagrożenia,</p> <p>i) zabezpieczenia lokalne chroniące cel zagrożenia,</p> <p>j) strefę bezpieczeństwa w której znajduje się cel zagrożenia.</p> <p>73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).</p> <p>74. 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.</p> <p>75. 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:</p> <p>a) nazwy zasobu,</p> <p>b) rodzaju zasobu,</p> <p>c) ważności zasobu dla organizacji,</p> <p>d) rodzaj przetwarzanych informacji,</p> <p>e) usług, które ten zasób świadczy,</p> <p>f) lokalizację użytkowników, którzy z niego korzystają,</p> <p>g) usługi z których zasób korzysta.</p> <p>76. 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.</p> <p>77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:</p> <p>a) nowe zdarzenie - jako zdarzenie zarejestrowane w systemie,</p>
--	--

	<p>b) segregacja - segregacja i kwalifikacja zdarzeń,</p> <p>c) incydent bezpieczeństwa - zdarzenie zakwalifikowane jako incydent bezpieczeństwa,</p> <p>d) fałszywy alarm - zdarzenie zakwalifikowane jako fałszywy alarm,</p> <p>e) zdarzenie obsługowane - zdarzenie, które zostało obsługowane w systemie.</p> <p>f) 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”.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.</p> <p>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 obsługiwany zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.</p> <p>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</p>
--	--

	<p>integracjami, m.in. loginy, hasła oraz klucze API.</p> <p>84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:</p> <ol style="list-style-type: none"> <li>podgląd aktywności zagrożonego zasobu na linii czasu,</li> <li>w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,</li> <li>w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,</li> <li>podgląd reguły korelacyjnej, która wygenerowała zdarzenie,</li> <li>w przypadku wykrytej techniki MITRE ATT&amp;CK® jej szczegółowy opis,</li> <li>listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,</li> <li>gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o: <ul style="list-style-type: none"> <li>listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,</li> <li>listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,</li> </ul> </li> <li>gotowe i proste w użyciu filtry rozszerzające analizę logów o: <ul style="list-style-type: none"> <li>listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,</li> <li>listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.</li> </ul> </li> </ol> <p>85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:</p> <ol style="list-style-type: none"> <li>warunki powiadomień, <ul style="list-style-type: none"> <li>zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,</li> <li>zdarzeń o przekroczonych czasach SLA o definiowalny okres,</li> <li>zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,</li> <li>zdarzeń, których priorytet osiągnął określoną wartość,</li> <li>zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,</li> <li>zdarzeń na których doszło do naruszenia bezpieczeństwa,</li> <li>zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,</li> <li>zdarzeń realizujących zdefiniowaną usługę,</li> <li>zdarzeń przetwarzających sklasyfikowane informacje,</li> <li>zdarzeń przetwarzanych na krytycznych zasobach,</li> </ul> </li> <li>odbiorców powiadomień, w tym: <ul style="list-style-type: none"> <li>operatora, któremu zostało przydzielone zdarzenie,</li> <li>właściciela zasobu na którym wystąpiło zdarzenie,</li> <li>zespół obsługi, który odpowiada za obsługę zdarzeń,</li> <li>właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,</li> <li>podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.</li> </ul> </li> <li>kanały powiadomień, m.in. e-mail, sms, komunikator,</li> <li>zastosowanie mechanizmów grupowania: <ul style="list-style-type: none"> <li>grupowanie wielu powiadomień w jednej wiadomości,</li> </ul> </li> </ol>
--	--

	<ul style="list-style-type: none"> <li>▪ ograniczenie liczby wierszy powiadomienia do określonej wartości.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>a) utworzenia nowego zdarzenia z określonym priorytetem,</li> <li>b) utworzenia nowego zdarzenia na zasobie krytycznym,</li> <li>c) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,</li> <li>d) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,</li> <li>e) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,</li> <li>f) modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,</li> <li>g) zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,</li> <li>h) przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.</li> </ul> <p>87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:</p> <ul style="list-style-type: none"> <li>a) wybór raportu, który ma zostać wysłany,</li> <li>b) zdefiniowanie jego tytułu,</li> <li>c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,</li> <li>d) możliwość ograniczenia cyklu do dni powszednich,</li> <li>e) określenie daty przesłania pierwszego raportu,</li> <li>f) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do: <ul style="list-style-type: none"> <li>▪ zdefiniowanej daty końcowej,</li> <li>▪ określonej liczby raportów,</li> </ul> </li> <li>g) określenie odbiorców raportu.</li> </ul> <p>88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).</p> <p>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:</p> <ul style="list-style-type: none"> <li>a) strefę bezpieczeństwa w której została wykryta podatność,</li> <li>b) prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,</li> <li>c) rodzaj zasobu którego dotyczy ta podatność,</li> <li>d) ważność tego zasobu dla organizacji,</li> <li>e) przetwarzane na tym zasobie informacje, np.: dane osobowe,</li> <li>f) usługi realizowane przez ten zasób, np.: DNS,</li> <li>g) wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,</li> <li>h) poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,</li> <li>i) szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej</li> </ul>
--	--

	<p>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.</p> <p>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 jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.</p> <p>91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:</p> <ul style="list-style-type: none"> <li>a) wyliczonym priorytecie podatności,</li> <li>b) aktualnym statusie obsługi,</li> <li>c) ważności zasobu na którym została wykryta,</li> <li>d) adresie IP tego systemu,</li> <li>e) parametrów SLA związanych z tym statusem,</li> <li>f) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,</li> <li>g) parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV)” = „Network”.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>a) przekroczenia czasu reakcji o określony czas np.: o godzinę,</li> <li>b) możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,</li> <li>c) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,</li> <li>d) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,</li> <li>e) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,</li> <li>f) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,</li> <li>g) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,</li> <li>h) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,</li> <li>i) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,</li> <li>j) przekroczenia czasu reakcji dla podatności na zasobie krytycznym,</li> <li>k) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,</li> </ul> <p>93. Dla obsługiwanym podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:</p> <ul style="list-style-type: none"> <li>a) warunki powiadomień,</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>▪ podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,</li> <li>▪ podatności o przekroczonych czasach SLA o definiowalny okres,</li> <li>▪ podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,</li> <li>▪ podatności, których priorytet osiągnął określoną wartość,</li> <li>▪ zdarzeń realizujących zdefiniowaną usługę,</li> <li>▪ zdarzeń przetwarzających sklasyfikowane informacje,</li> <li>▪ zdarzeń przetwarzanych na krytycznych zasobach,</li> </ul> <p>b) odbiorców powiadomień, w tym:</p> <ul style="list-style-type: none"> <li>▪ operatora, któremu została przydzielona podatność,</li> <li>▪ właściciela zasobu na którym wystąpiła podatność,</li> <li>▪ zespół obsługi, który odpowiada za obsługę podatności,</li> <li>▪ właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,</li> <li>▪ podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.</li> </ul> <p>c) kanały powiadomień, m.in. e-mail, sms, komunikator,</p> <p>d) zastosowanie mechanizmów grupowania:</p> <ul style="list-style-type: none"> <li>▪ grupowanie wielu powiadomień w jednej wiadomości,</li> <li>▪ ograniczenie liczby wierszy powiadomienia do określonej wartości.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>a) przydzielenia nowej podatności do obsługi z określonym priorytetem,</li> <li>b) przydzielenia nowej podatności do obsługi na zasobie krytycznym,</li> <li>c) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,</li> <li>d) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,</li> <li>e) modyfikacji przydzielonej operatorowi podatności przez innego operatora,</li> <li>f) zamknięcia przydzielonej operatorowi podatności przez innego operatora,</li> <li>g) przejęcia przydzielonej operatorowi podatności przez innego operatora.</li> </ul> <p>95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:</p> <ul style="list-style-type: none"> <li>a) wybór raportu który ma zostać wysłany,</li> <li>b) zdefiniowanie jego tytułu,</li> <li>c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,</li> <li>d) możliwość ograniczenia cyklu do dni powszednich,</li> <li>e) określenie daty przesłania pierwszego raportu,</li> <li>f) określenie okresu przez jaki będą one przesyłane, poprzez: <ul style="list-style-type: none"> <li>▪ zdefiniowanie daty końcowej,</li> </ul> </li> </ul>
--	---



	<ul style="list-style-type: none"> <li>▪ bez daty końcowej,</li> <li>▪ określenie liczby raportów,</li> </ul> <p>g) określenie odbiorców raportu.</p> <p>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.</p> <p>97. System musi pozwalać na tworzenie dedykowanych dashboard'ów obejmujących:</p> <ul style="list-style-type: none"> <li>a) zestaw wykresów dla bieżącego użytkownika,</li> <li>b) zestaw wykresów dla wybranego użytkownika,</li> <li>c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,</li> <li>d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).</li> </ul> <p>98. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy:</p> <ul style="list-style-type: none"> <li>a) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość zdarzeń nowych i niesklasyfikowanych,</li> <li>▪ ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,</li> <li>▪ ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,</li> </ul> </li> <li>b) wykres przedstawiający skalę zagrożeń, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość zasobów krytycznych na których są obsługiwane zdarzenia,</li> <li>▪ ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,</li> </ul> </li> <li>c) wykres przedstawiający źródła zagrożeń, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość nowych zdarzeń dotyczących użytkowników,</li> <li>▪ ilość podjętych zdarzeń dotyczących użytkowników,</li> <li>▪ ilość nowych zdarzeń dotyczących zasobów,</li> <li>▪ ilość podjętych zdarzeń dotyczących zasobów,</li> </ul> </li> <li>d) wykres przedstawiający poziom zagrożeń, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość nowych zdarzeń w podziale na priorytety,</li> <li>▪ ilość podjętych zdarzeń w podziale na priorytety,</li> </ul> </li> <li>e) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość zdarzeń zarejestrowanych w bieżącym dniu,</li> <li>▪ ilość zdarzeń zarejestrowanych w ostatnim tygodniu,</li> <li>▪ ilość zdarzeń zarejestrowanych w ostatnim miesiącu,</li> <li>▪ ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,</li> </ul> </li> <li>f) wykres przedstawiający zagrożone usługi, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,</li> <li>▪ ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,</li> </ul> </li> <li>g) wykres przedstawiający zagrożone dane, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,</li> <li>▪ ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,</li> <li>▪ ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,</li> </ul> </li> </ul>
--	---

	<ul style="list-style-type: none"> <li>▪ ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,</li> <li>h) wykres przedstawiający skalę podatności, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość zasobów krytycznych na których są obsługiwane podatności,</li> <li>▪ ilość zasobów niekrytycznych na których są obsługiwane podatności,</li> </ul> </li> <li>i) wykres przedstawiający czas obsługi podatności, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość podatności zarejestrowanych w bieżącym dniu,</li> <li>▪ ilość podatności zarejestrowanych w ostatnim tygodniu,</li> <li>▪ ilość podatności zarejestrowanych w ostatnim miesiącu,</li> <li>▪ ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,</li> </ul> </li> <li>j) wykres przedstawiający wagę podatności, który uwzględnia: <ul style="list-style-type: none"> <li>▪ ilość nowych podatności w podziale na priorytety,</li> <li>▪ ilość podjętych podatności w podziale na priorytety,</li> </ul> </li> </ul> <p>99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:</p> <ul style="list-style-type: none"> <li>a) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,</li> <li>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,</li> <li>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,</li> <li>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,</li> <li>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,</li> <li>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.</li> </ul> <p>100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.</p> <p>101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych</p>
--	--

	<p>dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:</p> <ul style="list-style-type: none"> <li>a) kolektor parsujący;</li> <li>b) kolektor logów;</li> <li>c) kolektor korelacyjny;</li> <li>d) kolektor zdarzeń;</li> <li>e) kolektor sztucznej inteligencji;</li> <li>f) kolektor reakcyjny;</li> <li>g) kolektor kontrolujący.</li> </ul> <p>102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.</p> <p>103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tys zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.</p> <p>104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.</p> <p>105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).</p> <p>106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.</p> <p>107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.</p> <p>108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość</p>
--	---

	<p>zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.</p> <p>109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszą być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.</p> <p>110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.</p> <p>111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.</p> <p>112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.</p> <p>113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tys zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.</p> <p>114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)</p> <p>115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.</p> <p>116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.</p> <p>117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.</p> <p>118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.</p> <p>119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do</p>
--	--

	<p>przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.</p> <p>120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).</p> <p>121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.</p> <p>122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów.</p> <p>123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)</p> <p>124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).</p> <p>125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:</p> <ul style="list-style-type: none"> <li>a) zdolność do definiowania wzorców które powtarzają się jako zmienne;</li> <li>b) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;</li> <li>c) zdolność do testowania poszczególnych funkcji;</li> <li>d) zdolność do przekształcania danych w trakcie ich parsowania.</li> </ul> <p>126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:</p> <ul style="list-style-type: none"> <li>a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;</li> <li>b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;</li> <li>c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;</li> <li>d) zdolność do monitorowania integralności plików;</li> <li>e) zdolność do monitorowania rejestru systemowego;</li> <li>f) zdolność do monitorowania urządzeń zewnętrznych (removable devices);</li> <li>g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;</li> <li>h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;</li> <li>i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;</li> <li>j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.</li> </ul> <p>127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity</p>
--	---



	<p>Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.</p> <p>128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI.</p> <p>129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Intelligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.</p> <p>130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).</p> <p>131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi.</p> <p>132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal.</p> <p>133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&amp;CK dla standardowego zbioru wbudowanych reguł.</p> <p>134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.</p> <p>135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.</p> <p>136. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.</p> <p>137. 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.</p> <p>138. 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.</p> <p>139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi</p>
--	--



	<p>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.</p> <p>140. 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.</p> <p>141. Produkt musi umożliwiać równoczesną pracę co najmniej 10 operatorów oraz obsługiwać min. 50 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.</p> <p>142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.</p> <p>143. 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.</p> <p>144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).</p> <p>145. Dostarczone rozwiązanie musi być objęte 24 miesięcznym 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).</p> <p>146. 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.</p>
Próbka systemu	<p>Zamawiający wymaga aby wraz z ofertą została dostarczona/udostępniona próbka systemu, która ma na celu weryfikację przez Zamawiającego wymagań OPZ. Rozwiązanie musi być skonfigurowane w sposób umożliwiający jego weryfikację z wymaganiami OPZ oraz musi pozwalać na zdalny dostęp. W ramach dostępu do rozwiązania, Wykonawca musi zapewnić wsparcie konsultanta technicznego oraz</p>

	<p>dostarczy odpowiednią dokumentację (np. w postaci karty produktu oraz niezbędnych instrukcji).</p> <p>Zamawiający maksymalnie w ciągu pięciu dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je z wymaganiami określonymi w powyższych punktach OPZ.</p> <p>W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona.</p>
--	---

## Zakup serwerów do pracy w klastrze wysokiej dostępności HA (High Availability Cluster)

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry rozwiązania jeśli są wymagane w formularzu ofertowym
Ilość	2 zestawy
Funkcjonalność obudowy	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości max 1U, wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack i wysuwanie serwera do celów serwisowych.</li> <li>Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</li> <li>Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.</li> </ul>
Funkcjonalność płyty głównej	Płyta główna wyposażona w: <ul style="list-style-type: none"> <li>16 slotów pamięci RAM przeznaczonych do instalacji pamięci RAM,</li> <li>Min. 3 sloty PCIe</li> <li>Min. 2 gniazda (sockets) pod procesory, zapewniająca obsługę procesorów 32 rdzeniowych</li> </ul>
Procesor	Zainstalowane dwa procesory wielordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 punktów w teście SPECrate2017_int_base dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla dwóch procesorów.  Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty raport z testu wydajności SPECrate@2017_int_base opublikowany na stronie <a href="http://www.spec.org">www.spec.org</a> dla oferowanego modelu serwera z oferowanym modelem procesora w konfiguracji dwuprocesorowej.
Pamięć RAM	256 GB pamięci RAM z możliwością rozbudowy do 1TB RAM.

	Wymagane funkcjonalności pamięci RAM: Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection.
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>2 interfejsy 1GbE w standardzie Base-T</li> <li>4 interfejsy 10/25GbE w standardzie SFP28</li> </ul>
Dyski twarde	Min. 2 dyski M.2 NVMe SSDs o pojemności min. 480GB każdy (Hot-Plug) z możliwością konfiguracji RAID 1.
Porty/złącza	<ul style="list-style-type: none"> <li>4x USB, w tym co najmniej 1x USB 3.0</li> <li>2x VGA</li> </ul>
Karta graficzna	Karta graficzna umożliwiająca pracę w rozdzielczości 1920x1200
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz Hot-Plug o mocy min. 1000W klasy Titanium (1+1)
Bezpieczeństwo	<ul style="list-style-type: none"> <li>Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.</li> <li>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>Moduł TPM 2.0</li> <li>Wymagana możliwość dynamicznego włączania i wyłączania portów USB na obudowie - bez potrzeby restartu serwera.</li> <li>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.</li> <li>Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</li> </ul>
Karta zarządzająca	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> <li>zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>wsparcie dla IPv6;</li> <li>wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li> <li>integracja z Active Directory;</li> <li>możliwość obsługi przez dwóch administratorów jednocześnie;</li> </ul>

	<ul style="list-style-type: none"> <li>▪ wsparcie dla dynamic DNS;</li> <li>▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;</li> <li>▪ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;</li> <li>▪ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: wirtualny schowek ułatwiający korzystanie z konsoli zdalnej, przesyłanie danych telemetrycznych w czasie rzeczywistym, dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze, automatyczną rejestrację certyfikatów (ACE).</li> </ul>
Oprogramowanie do zarządzania	<p>Wymagana możliwość zainstalowania oprogramowania do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> <li>▪ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.</li> <li>▪ Integracja z Active Directory.</li> <li>▪ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.</li> <li>▪ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.</li> <li>▪ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.</li> <li>▪ Szczegółowy opis wykrytych systemów oraz ich komponentów.</li> <li>▪ Możliwość eksportu raportu do CSV, HTML, XLS, PDF.</li> <li>▪ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>▪ Grupowanie urządzeń w oparciu o kryteria użytkownika.</li> <li>▪ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.</li> <li>▪ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.</li> <li>▪ Szybki podgląd stanu środowiska.</li> <li>▪ Podsumowanie stanu dla każdego urządzenia.</li> <li>▪ Szczegółowy status urządzenia/elementu/komponentu.</li> <li>▪ Generowanie alertów przy zmianie stanu urządzenia.</li> <li>▪ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.</li> <li>▪ Integracja z service desk producenta dostarczonej platformy sprzętowej.</li> <li>▪ Możliwość przejęcia zdalnego pulpitu.</li> <li>▪ Możliwość podmontowania wirtualnego napędu.</li> <li>▪ Kreator umożliwiający dostosowanie akcji dla wybranych alertów.</li> <li>▪ Możliwość importu plików MIB.</li> <li>▪ Przesyłanie alertów „as-is” do innych konsol firm trzecich.</li> <li>▪ Możliwość definiowania ról administratorów.</li> <li>▪ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.</li> <li>▪ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).</li> <li>▪ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.</li> </ul>

	<ul style="list-style-type: none"> <li>Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.</li> <li>Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li> <li>Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile.</li> <li>Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>Zdalne uruchamianie diagnostyki serwera.</li> <li>Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li> <li>Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul>
Gwarancja i serwis	<p>Zamawiający wymaga min. 2 lata (24 miesiące) gwarancji podstawowej na oferowane rozwiązanie.</p> <p>Zaoferowanie serwerów z gwarancją rozszerzoną (udzieloną przez producenta lub przez autoryzowanego partnera serwisowego producenta serwerów), wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla kryterium K1 - gwarancja serwerów do pracy w klastrze wysokiej dostępności HA (High Availability Cluster).</p> <p>Po potwierdzeniu spełnienia tego kryterium (przez wpisanie w formularzu ofertowym przez Wykonawcę informacji o długości gwarancji rozszerzonej), Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w pkt. 22 SWZ.</p>
Warunki gwarancji	<ul style="list-style-type: none"> <li>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li> <li>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych)</li> <li>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</li> <li>▪ Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>▪ Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej/ internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>▪ Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wsparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego).</li> <li>▪ Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego.</li> <li>▪ Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.</li> </ul>
Certyfikaty, normy i standardy	<ul style="list-style-type: none"> <li>▪ Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</li> <li>▪ Spełnianie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</li> <li>▪ Spełnianie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</li> <li>▪ Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.</li> <li>▪ Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części</li> </ul>



	<p>tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.</p> <p>Dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty wydruk ze strony internetowej <a href="http://www.epeat.net">www.epeat.net</a> potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.</p>
Komponenty	2x kabel direct attach 10GbE SFP+.

## Zakup licencji na serwerowy system operacyjny

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry rozwiązania jeśli są wymagane w formularzu ofertowym.
Ilość	2 licencje
Wymagania podstawowe	<ol style="list-style-type: none"> <li>Licencja na oprogramowanie musi zostać dostarczona do obsługi serwera fizycznego pracującego w klastrze HA, wyposażonego w 2 procesory 8-rdzeniowe. Jeśli dobór rodzaju lub liczby licencji zależy od liczby rdzeni procesora (procesorów) w serwerach, Wykonawca ma obowiązek dostarczyć właściwą liczbę licencji dla liczby rdzeni procesorów posiadanych przez Zamawiającego.</li> <li>Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym oraz nielimitowanej liczby środowisk serwerowego systemu operacyjnego.</li> <li>System musi być fabrycznie nowy (nie aktywowany wcześniej na innym urządzeniu).</li> <li>Zamawiający wymaga dostarczenia licencji na oprogramowanie (system serwerowy) w najnowszej wersji obecnie dostępnej na rynku</li> </ol>
Funkcjonalności, cechy	<p>Serwerowy system operacyjny musi posiadać następujące wymagania minimalne:</p> <ol style="list-style-type: none"> <li>Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.</li> <li>Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.</li> <li>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.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> </ol>

	<ol style="list-style-type: none"> <li>8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</li> <li>9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> <li>a) pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li> </ol> </li> <li>10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>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.</li> <li>12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET</li> <li>13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> <li>a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b) dotykowy umożliwiający sterowanie dotykem na monitorach dotykowych.</li> </ol> </li> <li>16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</li> <li>17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</li> <li>18. Mechanizmy logowania w oparciu o: <ol style="list-style-type: none"> <li>a) Login i hasło,</li> <li>b) Karty z certyfikatami (smartcard),</li> <li>c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> </ol> </li> <li>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.</li> <li>20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> <li>22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</li> <li>23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</li> <li>24. Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</li> </ol>
--	--

	<p>25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> <li>a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</li> <li>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: <ul style="list-style-type: none"> <li>▪ Podłączenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną,</li> <li>▪ Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania,</li> <li>▪ Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</li> <li>▪ Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.</li> </ul> </li> <li>c) Zdalna dystrybucja oprogramowania na stacje robocze.</li> <li>d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</li> <li>e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: <ul style="list-style-type: none"> <li>▪ Dystrybucję certyfikatów poprzez http</li> <li>▪ Konsolidację CA dla wielu lasów domeny,</li> <li>▪ Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,</li> <li>▪ Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</li> </ul> </li> <li>f) Szyfrowanie plików i folderów.</li> <li>g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</li> <li>h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</li> <li>i) Serwis udostępniania stron WWW.</li> <li>j) Wsparcie dla protokołu IP w wersji 6 (IPv6),</li> <li>k) Wsparcie dla algorytmów Suite B (RFC 4869),</li> <li>l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,</li> <li>m) budowane 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</li> </ul>
--	--

	<p>klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ul style="list-style-type: none"> <li>▪ Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</li> <li>▪ Obsługi ramek typu jumbo frames dla maszyn wirtualnych.</li> <li>▪ Obsługi 4-KB sektorów dysków</li> <li>▪ Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra</li> <li>▪ Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.</li> <li>▪ Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)</li> </ul> <p>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.</p> <p>27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p>
--	---

## Zakup licencji dostępowych CAL Device serwerowego systemu operacyjnego

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry rozwiązania jeśli są wymagane w formularzu ofertowym
Ilość	15 licencji
Wymagania ogólne	Wymagane jest dostarczenie licencji dostępu, która autoryzuje urządzenie końcowe w taki sposób aby urządzenie miało dostęp do serwera i mogło korzystać z usług serwera. Licencja musi być zgodna z wersją licencji na oferowany serwerowy system operacyjny.

## Zakup licencji dostępowych CAL User serwerowego systemu operacyjnego

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry rozwiązania jeśli są wymagane w formularzu ofertowym
Ilość	30 licencji

Wymagania ogólne	<p>Wymagane jest dostarczenie licencji dostępu, która autoryzuje osobę w taki sposób aby zalogowana osoba miała dostęp do aplikacji serwera i mogła korzystać z usług serwera z dowolnej liczby punktów końcowych.</p> <p>Licencja musi być zgodna z wersją licencji na oferowany serwerowy system operacyjny.</p>
------------------	--

## Zakup macierzy pamięci masowej (macierzy danych)

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry rozwiązania jeśli są wymagane w formularzu ofertowym
Ilość	1 zestaw
Obudowa	<ul style="list-style-type: none"> <li>Do instalacji w standardowej szafie Rack 19".</li> <li>Macierz musi zajmować wysokość maksymalnie 2U.</li> <li>Wymagana możliwość obsługi (instalacji) 24 dysków.</li> </ul>
Kontrolery	<ul style="list-style-type: none"> <li>Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active posiadające łącznie minimum 8 portów iSCSI z przepustowością minimum 25 Gb/s i udostępniające jednocześnie dane blokowe.</li> <li>Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.</li> <li>Komunikacja kontrolerów z podłączanymi półkami dyskowymi musi być realizowana przez połączenia SAS o przepustowości minimum 12 Gb/s.</li> </ul>
Cache	<ul style="list-style-type: none"> <li>Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.</li> <li>Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.</li> <li>Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.</li> <li>Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 4 TB z wykorzystaniem dysków SSD lub kart pamięci flash.</li> <li>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.</li> </ul>
Pamięć masowa	<p>Zainstalowane:</p> <ul style="list-style-type: none"> <li>12 dysków SAS 10k o pojemności 2,4TB każdy</li> <li>12 dysków SSD SAS o pojemności 1.92TB każdy</li> <li>Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".</li> <li>Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.</li> </ul>
Zabezpieczenie danych	<ul style="list-style-type: none"> <li>Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich</li> </ul>

	<p>kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).</p> <ul style="list-style-type: none"> <li>Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.</li> <li>Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).</li> <li>Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.</li> </ul>
Redundancja	<p>Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.</p> <p>Macierz musi umożliwiać wymianę elementów systemu w trybie „Hot-Swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.</p> <p>Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania - odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.</p> <p>Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.</p>
Funkcjonalności Oprogramowanie	<ul style="list-style-type: none"> <li>Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5.</li> <li>Wbudowany system powiadamiania drogą mailową o awarii.</li> <li>Macierz musi umożliwiać utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz.</li> <li>Wbudowana funkcjonalność automatycznego (bez interwencji człowieka) rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między różnymi typami dysków.</li> <li>Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.</li> <li>Rozwiązanie musi wspierać obsługę samoszyfrujących się dysków.</li> </ul> <p>Jeżeli którakolwiek z powyższych funkcjonalności wymaga dostarczenia dodatkowej licencji to należy ją zapewnić na całe oferowane rozwiązanie rozumiane w szczególności w zakresie przestrzeni dyskowej.</p>
Bezpieczeństwo	<p>Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania.</p> <p>Zasilacze, wentylatory, kontrolery RAID redundantne.</p>
Gwarancja i serwis	<p>Zamawiający wymaga min. 2 lata (24 miesiące) gwarancji podstawowej na oferowane rozwiązanie.</p> <p>Serwis będzie realizowany bezpośrednio przez producenta i/lub we współpracy z Partnerem Serwisowym Producenta w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.</p>



	<p>Zamawiający wymaga gwarancji uwzględniającej zabezpieczenie serwisowe, które w przypadku awarii dysku twardego (w urządzeniu objętym aktywnym wsparciem technicznym) powodującej konieczność jego wymiany, umożliwi pozostawienie uszkodzonego dysku u Zamawiającego (dysk nie będzie podlegał ekspertyzie poza siedzibą Zamawiającego).</p> <p>Wymagana możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji.</p> <ul style="list-style-type: none"> <li>Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.</li> <li>Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.</li> <li>W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników.</li> </ul> <p>Zaoferowanie macierzy z gwarancją rozszerzoną (udzieloną przez producenta lub przez autoryzowanego partnera serwisowego producenta macierzy), wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla kryterium K2 - gwarancja macierzy pamięci masowej (macierzy danych).</p> <p>W przypadku zaoferowania macierzy z gwarancją dodatkową okres zabezpieczenia serwisowego na nośniki pamięci masowej (dyski twarde), musi być równy udzielonej gwarancji rozszerzonej.</p> <p>Po potwierdzeniu spełnienia tego kryterium (przez wpisanie w formularzu ofertowym przez Wykonawcę informacji o długości gwarancji rozszerzonej), Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w pkt. 22 SWZ.</p>
Certyfikaty	<ul style="list-style-type: none"> <li>Spełnianie normy ISO 9001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</li> <li>Spełnianie normy ISO 14001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</li> <li>Spełnianie normy ISO 50001 lub równoważnej dla producenta sprzętu w zakresie produkcji - dokumentem potwierdzającym spełnienie wymagań będzie załączony do oferty certyfikat producenta.</li> </ul>
Komponenty	4x kabel direct attach 10GbE SFP+.

## Zakup urządzenia klasy UTM

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
---------	--

Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	1 zestaw
Wymagania ogólne	<p>Dostarczone rozwiązanie musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 5 administratorów do poszczególnych instancji systemu.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>▪ Firewall.</li> <li>▪ Ochrony w warstwie aplikacji.</li> <li>▪ Protokołów routingu dynamicznego.</li> </ul>
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> <li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji.</li> <li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li> <li>3. Monitoring stanu realizowanych połączeń VPN.</li> <li>4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</li> </ol>
Interfejsy, Zasilanie:	<ol style="list-style-type: none"> <li>1. System realizujący funkcję Firewall musi dysponować minimum: <ul style="list-style-type: none"> <li>▪ 10 portami Gigabit Ethernet RJ-45.</li> <li>▪ 2 gniazdami SFP 1 Gbps.</li> </ul> </li> <li>2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> <li>3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li> <li>4. System musi być wyposażony w zasilanie AC.</li> </ol>
Parametry wydajnościowe	<ol style="list-style-type: none"> <li>1. W zakresie Firewall'a obsługa nie mniej niż 1,4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.</li> <li>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</li> <li>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,7 Gbps.</li> <li>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.</li> </ol>

	<ol style="list-style-type: none"> <li>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,3 Gbps.</li> <li>6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.</li> <li>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 700 Mbps.</li> </ol>
Funkcje Systemu Bezpieczeństwa	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Zamawiający dopuszcza aby były one zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</li> <li>2. Kontrola Aplikacji.</li> <li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.</li> <li>4. Ochrona przed malware.</li> <li>5. Ochrona przed atakami - Intrusion Prevention System.</li> <li>6. Kontrola stron WWW.</li> <li>7. Kontrola zawartości poczty - Antyspam dla protokołów SMTP.</li> <li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</li> <li>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</li> <li>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</li> <li>12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</li> <li>13. Rozwiązanie musi posiadać wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</li> </ol>
Polityki, Firewall	<ol style="list-style-type: none"> <li>1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li> <li>2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> <li>▪ Translację jeden do jeden oraz jeden do wielu.</li> <li>▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li> </ul> </li> <li>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li> <li>4. Wymagana możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</li> <li>5. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</li> <li>6. Wymagana możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</li> </ol>

	<p>7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <ul style="list-style-type: none"> <li>▪ Amazon Web Services (AWS).</li> <li>▪ Microsoft Azure.</li> <li>▪ Cisco ACI.</li> <li>▪ Google Cloud Platform (GCP).</li> <li>▪ OpenStack.</li> <li>▪ VMware NSX.</li> <li>▪ Kubernetes.</li> </ul>
Połączenia VPN	<p>1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:</p> <ul style="list-style-type: none"> <li>▪ Wsparcie dla IKE v1 oraz v2.</li> <li>▪ Obsługę szyfrowania protokołem minimum AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM).</li> <li>▪ Obsługę protokołu Diffie-Hellman grup 19, 20.</li> <li>▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li> <li>▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li> <li>▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li> <li>▪ Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li> <li>▪ Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li> <li>▪ Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li> <li>▪ Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li> <li>▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li> </ul> <p>2. Na potrzeby przyszłej rozbudowy producent rozwiązania musi posiadać w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie VPN nie jest wymagane w implementacji.</p>
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ol style="list-style-type: none"> <li>1. Routingu statycznego.</li> <li>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).</li> <li>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.</li> <li>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li> <li>5. ECMP (Equal cost multi-path) - wybór wielu równoważnych tras w tablicy routingu.</li> <li>6. BFD (Bidirectional Forwarding Detection).</li> <li>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li> </ol>
Funkcje SD-WAN	<p>1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p>

	2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	<ol style="list-style-type: none"> <li>1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</li> <li>2. System musi dać możliwość określania pasma dla poszczególnych aplikacji.</li> <li>3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</li> <li>4. System musi zapewnić możliwość zarządzania pasmem dla wybranych kategorii URL.</li> </ol>
Ochrona przed malware	<ol style="list-style-type: none"> <li>1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</li> <li>3. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwiać konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</li> <li>4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</li> <li>5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</li> <li>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>7. System musi współpracować 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.</li> <li>8. Wymagana możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</li> <li>9. Wymagana możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</li> </ol>
Ochrona przed atakami	<ol style="list-style-type: none"> <li>1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</li> <li>2. System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.</li> <li>3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.</li> </ol>

	<ol style="list-style-type: none"> <li>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</li> <li>6. Wymagane mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</li> <li>7. Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</li> <li>8. Wymagana możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie</li> </ol>
Kontrola aplikacji	<ol style="list-style-type: none"> <li>1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</li> <li>2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</li> <li>4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</li> <li>5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.</li> <li>6. Wymagana możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>7. System musi umożliwiać określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</li> </ol>
Kontrola www	<ol style="list-style-type: none"> <li>1. Moduł kontroli WWW powinien korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</li> <li>2. W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</li> <li>3. Filtr WWW powinien dostarczać kategorii stron zabronionych prawem np.: Hazard.</li> <li>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.</li> <li>5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</li> <li>6. Filtr WWW ma dawać możliwość wykonania akcji typu „Warning” - ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</li> <li>7. Wymagana Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</li> <li>8. Administrator ma mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</li> <li>9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</li> </ol>



Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> <li>System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> <li>Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> </ul> </li> <li>Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</li> <li>Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</li> <li>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.</li> </ol>
Zarządzanie	<ol style="list-style-type: none"> <li>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.</li> <li>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania ma być realizowana z wykorzystaniem szyfrowanych protokołów.</li> <li>Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.</li> <li>System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</li> <li>System musi dać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</li> <li>Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</li> <li>Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</li> <li>Wymagana możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</li> <li>Wymagana możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</li> </ol>
Logowanie	<ol style="list-style-type: none"> <li>Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach dostawy musi zostać zapewniony (dostarczony) komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</li> <li>W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów - Zamawiający wymaga zapewnienia tej funkcjonalności w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026 r.</li> </ol>

	<p>3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.</p> <p>5. Musi istnieć możliwość logowania do serwera SYSLOG.</p> <p>6. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>7. Wymagana możliwość włączenia logowania per reguła w polityce firewall.</p> <p>8. System musi zapewniać możliwość logowania do serwera SYSLOG.</p> <p>9. Przesyłanie SYSLOG do zewnętrznych systemów będzie możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Testy wydajnościowe i testy funkcjonalne	<p>Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).</p>
Serwisy i licencje	<p>W ramach realizacji zadania Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Zamawiający wymaga zapewnienia tej funkcjonalności w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026r.</p> <p>Powinny one obejmować:</p> <ol style="list-style-type: none"> <li>1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.</li> <li>2. Licencja na usługę realizowaną w chmurze umożliwiającą logowanie i raportowanie z czasem retencji logów.</li> </ol>
Gwarancja i serwis	<p>Min. 2 lata (24 miesiące)</p>
Warunki gwarancji	<ul style="list-style-type: none"> <li>▪ System musi być objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.</li> <li>▪ W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</li> </ul>
Wsparcie techniczne dla systemu Firewall	<p>Zamawiający wymaga dostawy systemu objętego rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania, autoryzowany serwis producenta rozwiązania lub autoryzowanego dystrybutora przez okres udzielonej gwarancji.</p> <p>Dla dostarczonego rozwiązania Wykonawca zapewni usługę wsparcia technicznego świadczoną w języku polskim przez producenta lub Autoryzowanego Partnera Serwisowego Producenta w okresie udzielonej gwarancji w okresie realizacji projektu, tj. nie dłużej niż do 30.06.2026 co najmniej w następującym zakresie:</p> <ul style="list-style-type: none"> <li>▪ wsparcie telefoniczne zespołu certyfikowanych inżynierów,</li> </ul>

	<ul style="list-style-type: none"> <li>▪ pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu,</li> <li>▪ doradztwo w zakresie konfiguracji,</li> <li>▪ zdalne wsparcie techniczne,</li> <li>▪ pomoc w zakładaniu zgłoszeń serwisowych u producenta,</li> <li>▪ pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta,</li> <li>▪ przygotowanie urządzenia do zdalnej konfiguracji,</li> <li>▪ zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika,</li> <li>▪ minimum pięć zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika,</li> <li>▪ minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich</li> <li>▪ minimum dwa razy w roku zdalny upgrade oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich</li> </ul> <p>Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagany czas reakcji nie dłuższy niż 1 godzina - reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym</p>
Pozostałe wymagania	<p>1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p>

## Zakup zarządzalnego przełącznika sieciowego

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	2 zestawy
Obudowa	Rack 1U z elementami montażowymi do instalacji w szafie Rack
Obsługiwane warstwy	Warstwa trzecia
Ilość portów	48x 10/100/1000 PoE+ 4x 10 Gigabit SFP+

Przepustowość	170 Gbps
Wirtualna sieć lokalna (VLAN)	Tak

## Zakup serwera NAS z dyskami - typ 1

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	1 zestaw
Funkcjonalność obudowy	<ul style="list-style-type: none"> <li>Do instalacji w standardowej szafie typu Rack 19", serwer musi zajmować maksymalnie wysokość 2U, w zestawie szyny do montażu serwera w szafie typu Rack.</li> <li>Możliwość instalacji 12 dysków.</li> <li>Wyposażona w gniazda USB: 2x USB 3.2 Gen 2 (10 Gb/s)</li> <li>Wyposażona we wskaźniki LED informujące o statusach: HDD 1-12, LAN</li> </ul>
Procesor	Wymagany procesor wielordzeniowy, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 33.500 punktów. Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony <a href="http://www.cpubenchmark.net">www.cpubenchmark.net</a>
Pamięć operacyjna	min. 64 GB z możliwością rozbudowy do 192GB
Pamięć masowa	Dyski twarde klasy Enterprise przystosowane do zapisu ciągłego, zgodne z listą kompatybilności producenta oferowanego sprzętu, 10 sztuk o pojemności 10TB każdy.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
System plików	<ul style="list-style-type: none"> <li>Dyski wewnętrzne ZFS lub EXT4.</li> <li>Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+</li> </ul>
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
RAID	<ul style="list-style-type: none"> <li>Obsługiwane typy macierzy RAID: 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.</li> <li>Funkcje RAID: Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.</li> </ul>
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Interfejsy sieciowe	2x 2,5 GbE RJ-45 2x 10 GbE RJ-45 2x 10 GbE SFP+
Język GUI	Polski
Zasilanie	<ul style="list-style-type: none"> <li>Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz (1+1)</li> <li>Wymagana obsługa sieciowych awaryjnych zasilaczy UPS.</li> </ul>
Funkcja udostępniania plików	<ul style="list-style-type: none"> <li>Liczba kont użytkowników: 16000</li> <li>Liczba grup użytkowników: 500</li> <li>Liczba udziałów: 100</li> <li>Liczba jednoczesnych połączeń (CIFS): 5000</li> </ul>

	<ul style="list-style-type: none"> <li>Liczba migawek: 65000</li> </ul>
Gwarancja i serwis	<p>Zamawiający wymaga min. 2 lata (24 miesiące) gwarancji podstawowej na oferowane rozwiązanie.</p> <p>Zaoferowanie serwerów z gwarancją rozszerzoną (udzieloną przez producenta lub przez autoryzowanego partnera serwisowego producenta serwerów), wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla kryterium K3 - gwarancja serwera NAS typ 1.</p> <p>Po potwierdzeniu spełnienia tego kryterium (przez wpisanie w formularzu ofertowym przez Wykonawcę informacji o długości gwarancji dodatkowej), Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w pkt 22 SWZ.</p> <p>W ramach obsługi serwisowej Zamawiający wymaga zapewnienia:</p> <ul style="list-style-type: none"> <li>Wsparcia technicznego w przypadku problemów ze współpracą z innymi elementami sieci.</li> <li>Pełnej asysty telefonicznej (lub e-mailowej) przy aktualizacji oprogramowania.</li> <li>Pomocy technicznej w sprawach nietypowych, modyfikacjach oprogramowania itp.</li> <li>Priorytetowego trybu rozpatrywania gwarancji i prowadzenia naprawy.</li> </ul>
Komponenty	2x kabel direct attach 10GbE SFP+.

## Zakup serwera NAS z dyskami - typ 2

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	1 zestaw
Funkcjonalność obudowy	<ul style="list-style-type: none"> <li>Do instalacji w standardowej szafie typu Rack 19", serwer musi zajmować maksymalnie wysokość 2U, w zestawie szyny do montażu serwera w szafie typu Rack.</li> <li>Możliwość instalacji 12 dysków HDD oraz 2 dysków M.2 SSD</li> <li>Wyposażona w gniazda USB: 2x USB 3.2 Gen 2 (10 Gb/s)</li> <li>Wyposażona we wskaźniki LED informujące o statusach: HDD 1-12, M.2 SSD 1-2, LAN</li> </ul>
Procesor	Wymagany procesor wielordzeniowy, umożliwiający osiągnięcie w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik min. 22.500 punktów. Dokumentem potwierdzającym spełnienie wymagań będzie złożony przez Wykonawcę wydruk ze strony <a href="http://www.cpubenchmark.net">www.cpubenchmark.net</a>
Pamięć operacyjna	min. 32 GB z możliwością rozbudowy do 192GB
Pamięć masowa	Dyski twarde klasy Enterprise przystosowane do zapisu ciągłego, zgodne z listą kompatybilności producenta oferowanego sprzętu, 10 sztuk o pojemności 10TB każdy.

Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
System plików	<ul style="list-style-type: none"> <li>Dyski wewnętrzne ZFS lub EXT4.</li> <li>Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+</li> </ul>
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
RAID	<ul style="list-style-type: none"> <li>Obsługiwane typy macierzy RAID: 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.</li> <li>Funkcje RAID: Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.</li> </ul>
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Interfejsy sieciowe	2x 2,5 GbE RJ-45 2x 10 GbE RJ-45 2x 10 GbE SFP+
Język GUI	Polski
Zasilanie	<ul style="list-style-type: none"> <li>Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz (1+1)</li> <li>Wymagana obsługa sieciowych awaryjnych zasilaczy UPS.</li> </ul>
Funkcja udostępniania plików	<ul style="list-style-type: none"> <li>Liczba kont użytkowników: 16000</li> <li>Liczba grup użytkowników: 500</li> <li>Liczba udziałów: 100</li> <li>Liczba jednoczesnych połączeń (CIFS): 5000</li> <li>Liczba migawek: 65000</li> </ul>
Gwarancja i serwis	<p>Zamawiający wymaga min. 2 lata (24 miesiące) gwarancji podstawowej na oferowane rozwiązanie.</p> <p>Zaoferowanie serwerów z gwarancją rozszerzoną (udzieloną przez producenta lub przez autoryzowanego partnera serwisowego producenta serwerów), wydłużającą gwarancję podstawową o okres dodatkowych 12, 24, 36 lub więcej miesięcy jest wymogiem nieobowiązkowym (fakultatywnym) i jest kryterium dodatkowo punktowanym zgodnie z kryterium oceny ofert dla kryterium K4 - gwarancja serwera NAS typ 2.</p> <p>Po potwierdzeniu spełnienia tego kryterium (przez wpisanie w formularzu ofertowym przez Wykonawcę informacji o długości gwarancji dodatkowej), Wykonawcy zostanie przyznana liczba punktów określona w pozostałych kryteriach oceny ofert zgodnie z kryteriami określonymi w pkt 22 SWZ.</p> <p>W ramach obsługi serwisowej Zamawiający wymaga zapewnienia:</p> <ul style="list-style-type: none"> <li>Wsparcia technicznego w przypadku problemów ze współpracą z innymi elementami sieci.</li> <li>Pełnej asysty telefonicznej (lub e-mailowej) przy aktualizacji oprogramowania.</li> <li>Pomocy technicznej w sprawach nietypowych, modyfikacjach oprogramowania itp.</li> <li>Priorytetowego trybu rozpatrywania gwarancji i prowadzenia naprawy.</li> </ul>
Komponenty	2x kabel direct attach 10GbE SFP+.



## Zakup oprogramowania do realizacji kopii zapasowych ze wsparciem w okresie realizacji projektu

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	1 zestaw
Wymagania ogólne	<ol style="list-style-type: none"> <li>Oprogramowanie musi zapewnić realizację kopii zapasowych z dwóch serwerów fizycznych i dwunastu maszyn wirtualnych.</li> <li>Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne w okresie realizacji projektu do 30.06.2026 r.</li> <li>Oprogramowanie musi współpracować z infrastrukturą VMware oraz Microsoft Hyper-V. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.</li> <li>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.</li> </ol>
Całkowite koszty posiadania	<ol style="list-style-type: none"> <li>Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.</li> <li>Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.</li> <li>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</li> <li>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.</li> <li>Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.</li> <li>Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.</li> <li>Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</li> <li>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania</li> </ol>

	<ol style="list-style-type: none"> <li>9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)</li> <li>10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu</li> <li>11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API</li> <li>12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji</li> <li>13. 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</li> <li>14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania</li> <li>15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</li> <li>16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej</li> <li>17. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)</li> <li>18. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)</li> <li>19. Oprogramowanie musi posiadać integracje z systemami typu SIEM</li> <li>20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.</li> </ol>
Wymagania RPO	<ol style="list-style-type: none"> <li>1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej</li> <li>2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</li> <li>3. 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 z dokładnością do pojedynczego datastora</li> <li>4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</li> <li>5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</li> </ol>

	<ol style="list-style-type: none"> <li>6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).</li> <li>7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)</li> <li>8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.</li> <li>9. 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.</li> <li>10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</li> <li>11. 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.</li> <li>12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</li> <li>13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik</li> <li>14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)</li> <li>15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)</li> </ol>
Wymagania RTO	<ol style="list-style-type: none"> <li>1. 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, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.</li> <li>2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</li> <li>3. 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</li> <li>4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre</li> </ol>

5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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
9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
17. 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.
18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

	<ol style="list-style-type: none"> <li>19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji</li> <li>20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN</li> <li>21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle</li> <li>22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI</li> <li>23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2</li> <li>24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</li> </ol>
Ograniczenie ryzyka	<ol style="list-style-type: none"> <li>1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</li> <li>2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</li> <li>3. 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</li> <li>4. 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.</li> <li>5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware</li> <li>6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania</li> <li>7. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków</li> <li>8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</li> </ol>
Środowiska fizyczne	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego</li> <li>2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych</li> </ol>



3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4. Rozwiązanie musi wspierać system operacyjny macOS
5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
9. Rozwiązanie musi wspierać backup podłączonych dysków USB
10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
12. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13. Rozwiązanie musi wspierać kontrolę pasma sieciowego
14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17. Rozwiązanie musi wspierać technologię BitLocker
18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorzędowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
23. Rozwiązanie musi wspierać szyfrowanie



	<p>24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne</p> <p>25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego</p> <p>26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej</p> <p>27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych</p>
Monitoring	<p>1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich</p> <p>2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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.</p> <p>4. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter</p> <p>5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn</p> <p>6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel</p> <p>7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk</p> <p>8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora</p> <p>9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów</p> <p>10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)</p> <p>11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna</p> <p>12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego</p> <p>13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta</p> <p>14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.</p> <p>15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów</p>

	<p>konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.</p> <p>16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware</p> <p>17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4</p>
Raportowanie	<p>1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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.</p> <p>3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.</p> <p>4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V</p> <p>5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF</p> <p>6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc</p> <p>7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach</p> <p>8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów</p> <p>9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych</p> <p>10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych</p> <p>11. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury</p> <p>12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta</p> <p>13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.</p> <p>14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.</p> <p>15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware</p>

	<p>16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)</p> <p>17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie</p>
--	--

## Zakup dysków zewnętrznych USB w celu przechowywania odseparowanych od sieci kopii zapasowych

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	2 zestawy
Pojemność	10TB
Złącze	USB 3.0
Bezpieczeństwo	256-bitowe szyfrowanie danych AES
Gwarancja i serwis	Min. 2 lata (24 miesiące)

## Zakup zasilaczy awaryjnych UPS typu Rack

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	2 zestawy
Obudowa	Typu Rack, wysokość 2U, w zestawie szyny montażowe do szafy Rack 19"
Technologia	TRUE ON LINE Double Conversion
Moc znamionowa	3 kVA / 3 kW
Wyjściowy współczynnik mocy (PF)	1,0
Napięcie wejściowe	230 Vac
Sposób zasilania	Plug&Play Gniazdo w standardzie IEC 320
Tolerancja napięcia wejściowego	161 – 299 V przy obciążeniu 50-100%; bez przechodzenia na baterie 115 – 299 Vac przy obciążeniu mniejszym od 50%; bez przechodzenia na baterie
Częstotliwość wejściowa	Wymagana 50 Hz +/-20%
Sprawność AC-AC	<ul style="list-style-type: none"> <li>nie mniejsza niż 93% w trybie pracy on-line z obciążeniem 100%</li> <li>nie mniejsza niż 99% w trybie pracy Oszczędzania energii Eco Mode</li> </ul>
Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.

Napięcie wyjściowe	230 V
Częstotliwość wyjściowa	50/60Hz (programowalna)
Zintegrowane bezprzerwowe przełączniki obejściowy Bypass	Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny
Czas podtrzymania (wg karty katalogowej producenta)	<ul style="list-style-type: none"> <li>nie mniej niż 4 minuty przy 100% obciążenia</li> <li>nie mniej niż 11 minut przy 50% obciążenia</li> </ul>
Złącze baterii zewnętrznych	<p>Musi istnieć możliwość dołączenia jednostki rozszerzającej wyposażonej w dodatkowe łańcuchy baterii (moduł baterii) wydłużające czas podtrzymania zasilania. Zamawiający wymaga zapewnienia czasu podtrzymania przy zastosowaniu baterii wewnętrznych oraz modułu baterii zewnętrznych dla następujących obciążeń zasilacza (wg danych z karty katalogowej producenta):</p> <ul style="list-style-type: none"> <li>przy 50% obciążeniu nie mniej niż 47 minut</li> <li>przy 100% obciążeniu nie mniej niż 20 minut</li> </ul>
Akumulatory	<ul style="list-style-type: none"> <li>Szczelne, bezobsługowe, technologia AGM, o projektowanej żywotności min. 10 lat,</li> <li>Baterie w UPS do wymiany w trybie HotSwap oraz możliwość odłączenia modułu bateryjnego za pomocą wtyczki</li> </ul>
Układ ładowania akumulatorów o konfigurowalnych parametrach	Możliwość ładowania akumulatorów prądem w zakresie 1 – 8A konfigurowalnym z LCD (bez konieczności stosowania oprogramowania serwisowego)
Stabilizacja napięcia wyjściowego	<ul style="list-style-type: none"> <li>w stanie ustalonym <math>\pm 1\%</math></li> <li>w stanie nieustalonym <math>\pm 3\%</math></li> </ul>
Stabilność częstotliwości wyjściowej:	bez synchronizacji: $\pm 0,1\%$
Współczynnik szczytu	3:1
Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną	Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości, pozostałego czasu pracy podczas pracy bateryjnej.
Interfejsy	<p>Złącze interfejsów komunikacyjnych: RS232, USB, slot SNMP</p> <p>Interfejs EPO (do wyłącznika ppoż.)</p>
Gniazda wyjściowe IEC320 na zasilaczu UPS	Wymagane minimum gniazd: 8x 10A oraz 1x 16A

Oprogramowanie	Wymagane oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego.
Poziom hałasu w odległości 1m,	< 48 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
Możliwość regulacji z oprogramowania tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Regulacja z Panela LCD
Wyposażenie dodatkowe	Wraz z zasilaczem musi zostać dostarczona karta SNMP do zarządzania UPS z poziomu sieci.
Gwarancja i serwis	Min. 2 lata (24 miesiące)

## Zakup zasilaczy awaryjnych UPS do stanowisk komputerowych

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	26 zestawów
Obudowa	Typu Tower
Technologia	TRUE ON LINE Double Conversion
Moc znamionowa	1kVA / 0,9kW
Wyjściowy współczynnik mocy	0,9
Funkcje	Start z baterii (zimny start) Panel kontrolny LCD informujący o trybie pracy, parametrach zasilacza, zapewniający konfigurację parametrów UPS. Automatyczna diagnostyka zapewniająca pełną sprawność urządzenia, kontrolę podzespołów i parametrów pracy bez konieczności ingerencji użytkownika.
Poziom hałasu	<49 dB
Gniazda wyjściowe IEC320 na zasilaczu UPS	Wymagane minimum 3 gniazda
Gwarancja i serwis	Min. 2 lata (24 miesiące)

## Zakup utrzymania wsparcia technicznego wraz z subskrypcjami dla posiadanego UTM

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
---------	--

Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	1 zestaw
Rodzaj wsparcia z subskrypcjami	<p>W celu zapewnienia aktualnej ochrony sieci wewnętrznej, Zamawiający wymaga dostarczenia pakietów licencji dotyczących wsparcia technicznego wraz z subskrypcjami dla wymienionych funkcji bezpieczeństwa powiązanych z posiadanym urządzeniem UTM Stormshield SN210:</p> <ol style="list-style-type: none"> <li>1. Stormshield UTM SN210 UTM Security Pack (FW+IPS, VPN, URL, AV, AS)</li> <li>2. Stormshield UTM SN210 Next Business Day</li> </ol> <p>Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne w okresie realizacji projektu, do 30.06.2026 r.</p>

## Zakup utrzymania wsparcia technicznego wraz z subskrypcjami dla posiadanego systemu do zarządzania zasobami IT

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Dane do formularza ofertowego	W ofercie należy wskazać producenta, model (symbol) oferowanego rozwiązania oraz podstawowe parametry wymagane (określone) w formularzu ofertowym
Ilość	1 zestaw
Rodzaj wsparcia	<p>W celu zapewnienia aktualnego wsparcia, Zamawiający wymaga dostarczenia aktualizacji wsparcia technicznego wraz z subskrypcjami dla posiadanej licencji oprogramowania od zarządzania zasobami i procesami IT pod nazwą „IT Manager” firmy Infonet Projekt S.A.</p> <p>Licencje oraz serwisy powinny mieć zapewnione wsparcie techniczne (polisę serwisową) gwarantującą świadczenie usługi supportu w okresie realizacji projektu, do 30.06.2026 r. wraz z dostępem do nowych wersji systemu w ramach posiadanych modułów systemu ITManager.</p> <p>Zamawiający informuje, że wymaga dostawy suportu dla pakietu obejmującego moduły:</p> <ol style="list-style-type: none"> <li>a) Baza konfiguracji komputerów oraz oprogramowania</li> <li>b) Zarządzanie licencjami, audyt oprogramowania</li> <li>c) Zdalny pulpit, zdalne zarządzanie komputerem</li> <li>d) Monitoring użytkowników</li> <li>e) Zarządzanie urządzeniami USB storage</li> <li>f) Backup Danych Użytkownika</li> <li>g) Zarządzanie Zadaniem, Zarządzanie Polisan, Grupy Dynamiczne</li> </ol> <p>Oraz dodatki:</p> <ol style="list-style-type: none"> <li>a) Zarządzanie zasobami oraz użytkownikami</li> <li>b) ServiceDesk (Server: Lite; ilość UserCal: 31), zarządzanie wnioskami, zarządzanie uprawnieniami</li> <li>c) Aktywny monitoring sieci LAN (Server: Lite; ilość DeviceCal: 31)</li> <li>d) Komunikator (Server: Lite; ilość DeviceCal: 31)</li> </ol>



## Zakup usług konfiguracyjnych pozwalających wdrożyć nowe rozwiązania informatyczne

ATRYBUT	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE LUB FUNKCJONALNE
Założenia ogólne	<p>Celem prac jest przygotowanie środowiska teleinformatycznego w Urzędzie Gminy w Kamieniu w oparciu o dostarczone rozwiązania sprzętowe i oprogramowanie. Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielami Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia oraz umożliwi Wykonawcy dostęp do infrastruktury w ustalonym terminie w celu przygotowania procedur wdrożenia. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego. Po zapoznaniu się z architekturą sieciową urzędu Wykonawca przedstawi plan reorganizacji sieci oraz wirtualizacji z uwzględnieniem istniejącego i dostarczanego sprzętu. Schemat ten musi być uzgodniony z Zamawiającym i uwzględniać jego wytyczne.</p> <p>Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych.</p>
Montaż i fizyczne uruchomienie systemu	<p>Zamawiający wymaga zainstalowania dostarczonych urządzeń we wskazanym pomieszczeniu w następującym zakresie:</p> <ol style="list-style-type: none"> <li>1. Wniesienie i fizyczny montaż urządzeń w szafie typu Rack.</li> <li>2. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.</li> <li>3. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.</li> <li>4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.</li> <li>5. Dla urządzeń modułowych wymagany jest montaż i instalacja wszystkich podzespołów.</li> <li>6. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji - Wykonawca zapewni niezbędne okablowanie, m.in. patchordy miedziane (min. kat. 6 UTP) lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym.</li> <li>7. Po wykonaniu instalacji, wymagane jest przeprowadzenie testów sprawdzających poprawność instalacji i działania urządzeń.</li> </ol>
Reorganizacja i porządkowanie	<p>Po zapoznaniu się z architekturą sieciową urzędu i przedstawieniu Zamawiającemu schematu reorganizacji sieci (z uwzględnieniem istniejącego i dostarczanego sprzętu), Wykonawca przeprowadzi porządkowanie połączeń wewnętrznych.</p>
Konfiguracja przełączników sieci LAN	<p>Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi urządzeniami sieciowymi. Przełączniki będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego). Wykonawca przeprowadzi konfigurację dostarczanych przełączników w zakresie:</p> <ol style="list-style-type: none"> <li>1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.</li> <li>2. W celu odseparowania różnego typu ruchu sieciowego wymagana jest konfiguracja sieci wirtualnych VLAN - schemat ten musi być uzgodniony z Zamawiającym i uwzględniać jego wytyczne.</li> </ol>

	<ol style="list-style-type: none"> <li>3. Konfiguracja połączeń pomiędzy istniejącymi przełącznikami.</li> <li>4. Konfiguracja routingu pomiędzy sieciami VLAN na firewall'u.</li> <li>5. Testowanie obsługi ruchu sieciowego oraz testowanie skuteczności zabezpieczeń.</li> </ol>
Konfiguracja urządzenia klasy UTM	<ol style="list-style-type: none"> <li>1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.</li> <li>2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.</li> <li>3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)</li> <li>4. Przygotowanie projektu włączenia urządzenia do sieci LAN Urzędu Gminy</li> <li>5. Konfiguracja dostarczonego systemu Firewall: <ol style="list-style-type: none"> <li>a. Konfiguracja podstawowych parametrów</li> <li>b. Konfiguracja translacji adresów NAT</li> <li>c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, serwery komunikacyjne telefonii IP, itp.</li> <li>d. Konfiguracja inspekcji określonych protokołów sieciowych;</li> <li>e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;</li> <li>f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;</li> <li>g. Testowanie działania bramy</li> </ol> </li> <li>6. Konfiguracja modułów należących do systemu wykrywania włamań IPS: <ol style="list-style-type: none"> <li>a. Konfiguracja podstawowych parametrów</li> <li>b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;</li> <li>c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;</li> <li>d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;</li> <li>e. Testowanie działania ochrony IPS</li> </ol> </li> <li>7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. <ol style="list-style-type: none"> <li>a. Przypisanie adresu IP do zarządzania.</li> <li>b. Konfiguracja inspekcji protokołów HTTP, SMTP, FTP, POP3</li> <li>c. Definicja reguł filtrowania/blokowania</li> </ol> </li> <li>8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej z uwierzytelnieniem w oparciu o usługę katalogową.</li> <li>9. Uruchomienie i skonfigurowanie instancji systemów bezpieczeństwa dla skonfigurowanych sieci wirtualnych VLAN, taka liczba sieci wirtualnych aby odseparować różne typy ruchu, w porozumieniu z zamawiającym.</li> <li>10. W instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekazuje Zamawiający) dla każdej z poniższych funkcjonalności: <ol style="list-style-type: none"> <li>a. kontrola dostępu - zaporą ogniową klasy Stateless Inspection</li> </ol> </li> </ol>

	<ul style="list-style-type: none"> <li>b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar</li> <li>c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]</li> <li>d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.</li> <li>e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)</li> <li>f. kontrola pasma oraz ruchu [QoS, Traffic shaping]</li> <li>g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P</li> <li>h. Ochrona przed wyciekiem poufnej informacji (DLP)</li> <li>i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)</li> <li>j. Inspekcja ruchu SSL</li> <li>k. Ochrony przed atakami na stacje klienckie</li> <li>l. Kontrola pasma</li> </ul> <p>11. Konfiguracja logowania i raportowania.</p> <p>12. Konfiguracja logowania i raportowania do alternatywnego serwera SYSLOG uruchomionego na serwerze NAS (instalacja i konfiguracja serwera SYSLOG spoczywa na Wykonawcy). Jeśli dla zapewnienia tej funkcjonalności wymagane są jakiegokolwiek licencje - ich dostarczenie spoczywa na Wykonawcy.</p>
Instalacja i konfiguracja serwerów, instalacja systemu operacyjnego	Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane, a następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
Wirtualizacja dla serwerów	<p>Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w następującym zakresie:</p> <ol style="list-style-type: none"> <li>1. Aktywacja licencji oprogramowania wirtualizacyjnego.</li> <li>2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego - aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.</li> <li>3. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach.</li> <li>4. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.</li> <li>5. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego.</li> </ol> <p>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) <math>n-(n-1)</math> ścieżek, gdzie <math>n</math> oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.</p>

	<p>6. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) <math>n-(n-1)</math> ścieżek, gdzie <math>n</math> oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.</p> <p>7. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.</p> <p>8. Przygotowania koncepcji i wykonania wirtualizacji maszyn w liczbie uzgodnionej z Zamawiającym.</p> <p>9. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.</p> <p>10. Konfiguracja klastra wysokiej dostępności:</p> <ol style="list-style-type: none"> <li>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.</li> <li>Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.</li> <li>Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.</li> </ol> <p>11. Weryfikacja działania klastra wysokiej dostępności.</p>
Usługa katalogowa	<p>W ramach uruchomienia usługi należy przeprowadzić migrację dwóch grup użytkowników domenowych działających w środowisku Zamawiającego do nowego systemu.</p> <p>Usługa katalogowa musi być uruchomiona wraz z komponentami odpowiedzialnymi za rozwiązywanie nazw - należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowany system operacyjny, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.</p> <p>Usługa powinna uwzględniać strukturę jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.</p> <p>Zalecane jest wdrożenie globalnej polityki haseł spełniających zasady złożoności - Szczegółowe dane zostaną przekazane na etapie konfiguracji.</p> <p>Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:</p> <ol style="list-style-type: none"> <li>Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości</li> <li>Śledzenie zmian dotyczących tworzenia, usuwania obiektów</li> </ol> <p>Zamawiający wymaga skonfigurowania jednej stacji zarządzającej. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).</p>

Serwery NAS	Zamawiający wymaga skonfigurowania i uruchomienia serwerów NAS w taki sposób aby pierwszy z NAS był przeznaczony do składowania kopii zapasowych, drugi natomiast ma być przeznaczony pod pliki użytkowników. W przypadku urządzenia pod pliki użytkowników wymagana jest migracja danych (przeniesienie katalogów domowych) ze starego NAS do nowego NAS.
Kopie zapasowe	<p>Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych (przy współudziale serwera NAS) oraz aktywacja wymaganych licencji.</p> <p>Wymagana będzie konfiguracja zadań wykonywania kopii zapasowych przy wykorzystaniu serwera NAS i oprogramowania do niego przypisanego:</p> <ol style="list-style-type: none"> <li>1. Kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące.</li> <li>2. Kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy.</li> <li>3. Kopie maszyn wirtualnych muszą być replikowane na wskazany przez Zamawiającego zasób dyskowy.</li> <li>4. Kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu.</li> <li>5. Kopie zapasowe muszą (jeżeli jest taka funkcjonalność) być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową.</li> <li>6. Musi istnieć możliwość odtworzenia: całej wirtualnej maszyny, dysku wirtualnej maszyny, pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa).</li> </ol> <p>Oprogramowanie musi umożliwiać:</p> <ol style="list-style-type: none"> <li>1. Replikację maszyn wirtualnych w oparciu o obrazy.</li> <li>2. Syntetyczną pełną kopię zapasową - tworzenie kopii zapasowych forever-incremental.</li> <li>3. Tworzenie harmonogramów kopii zapasowych bezpośrednio z UI.</li> <li>4. Weryfikacja kopii zapasowej pod kątem infekcji i złośliwego oprogramowania przed przywróceniem do środowiska produkcyjnego.</li> <li>5. Konfiguracja powiadomień o wykonaniu kopii zapasowej (e-mail).</li> </ol>
SIEM / SOAR	Zamawiający wymaga przeprowadzenie wdrożenia w środowisku informatycznym urzędu systemu przeciwdziałającego cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.
Szkolenie	<p>Wykonawca przeprowadzi w siedzibie Zamawiającego podstawowe szkolenie dla Administratorów systemu. Szkoleniem zostaną objęte osoby wskazane przez Zamawiającego z zakresie dostarczonego rozwiązania teleinformatycznego, co najmniej w zakresie:</p> <ol style="list-style-type: none"> <li>1. Obsługi dostarczonych serwerów, macierzy dyskowej oraz utrzymania klastra HA.</li> <li>2. Obsługi dostarczonego rozwiązania do backupu, archiwizacji danych oraz wykonywania kopii zapasowych.</li> <li>3. Zarządzania przełącznikami sieciowymi.</li> </ol>

	Celem szkolenia administratorów będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce. Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie.
Opracowanie dokumentacji technicznej, Odbiory	Zamawiający wymaga opracowania dokumentacji technicznej użytkownika (dokumentacji powykonawczej) w formie papierowej i elektronicznej. Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z dokumentacją.