

## Opis Przedmiotu Zamówienia (OPZ)

### I. Zakup oprogramowania systemowego zwanego SSO wraz z licencjami dostępowymi

---

#### 1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa fabrycznie nowych, oryginalnych i nieużywanych licencji oraz uprawnień dostępowych, obejmujących:

- 4 sztuki oprogramowania systemowego SSO rodzaju datacenter, zgodnego z aktualną ofertą producenta i wspieranego technicznie w dniu dostawy.
- 150 sztuk licencji dostępowych Client Access License przeznaczonych dla użytkowników końcowych.

Dostarczone oprogramowanie ma umożliwiać:

- uruchomienie i zarządzanie środowiskiem wirtualnym (w tym dowolną liczbą maszyn wirtualnych na licencjonowanym hoście),
  - budowę lub rozbudowę lokalnej domeny Active Directory,
  - stosowanie zaawansowanych polityk bezpieczeństwa zgodnych z wytycznymi **KRI (Krajowe Ramy Interoperacyjności)**,
  - centralne zarządzanie użytkownikami, grupami, politykami GPO oraz zabezpieczeniami serwerowymi.
- 

#### 2. Wymagania

Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Wymagane są licencje na wszystkie rdzenie.

SSO musi posiadać następujące, wbudowane cechy:

- 1) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
- 2) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
- 3) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,

- 4) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
- 5) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
- 6) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
- 7) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
- 8) wbudowane wsparcie instalacji i pracy na wolumenach, które:
  - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
  - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
  - c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
  - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL),
- 9) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
- 10) wbudowane szyfrowanie dysków,
- 11) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
- 12) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
- 13) graficzny interfejs użytkownika,
- 14) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- 15) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
- 16) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
- 17) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
- 18) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji,
- 19) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
- 20) 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:

- a) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
- b) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
- c) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
- d) zdalna dystrybucja oprogramowania na stacje robocze,
- e) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,

21) centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego, umożliwiające:

- a) dystrybucję certyfikatów poprzez http,
- b) konsolidację CA dla wielu lasów domeny,
- c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- d) szyfrowanie plików i folderów,
- e) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),

22) wbudowane mechanizmy wirtualizacji (Hypervisor) zapewniające wsparcie dla:

- a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- b) obsługi ramek typu jumbo frames dla maszyn wirtualnych,
- c) obsługi 4-KB sektorów dysków,
- d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
- e) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
- f) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),

23) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,

24) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),

25) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,

26) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,

- 
- 27) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 28) SSO musi posiadać oficjalne wsparcie producenta co najmniej do roku 2034 oraz być wydany nie wcześniej niż w 2024 roku, z wbudowaną funkcjonalnością aktualizacji bez restartu systemu (hotpatching) dla krytycznych poprawek bezpieczeństwa.
- 

#### 4. Wymagania formalne

- Licencje muszą pochodzić z oficjalnego kanału sprzedaży i być objęte wsparciem producenta.
  - Oprogramowanie musi być zgodne z obowiązującymi przepisami dotyczącymi interoperacyjności i cyberbezpieczeństwa.
  - Wykonawca musi zapewnić pomoc w zakresie aktywacji i ewentualnego przypisania licencji do konta Zamawiającego.
  - Zamawiający nie jest objęty zniżkami licencyjnymi EDU, GOV, NPO
  - Licencje nie mogą pochodzić z rynku licencji używanych, nie mogą być wcześniej aktywowane. Zamawiający zastrzega sobie prawo do weryfikacji zgodności tych zapisów z odpowiednim działem producenta.
  - Wykonawca musi zapewnić komplet dokumentów potwierdzający legalność nabytego oprogramowania, tj. Fakturę zakupu z oficjalnego kanału dystrybucji, pełną dokumentację legalności oprogramowania, oświadczenie wykonawcy o zgodności oprogramowania z obecnym prawem i możliwością użytkowania na terenie Unii Europejskiej.
- 

#### 5. Termin realizacji

Maksymalnie **30 dni kalendarzowych** od dnia podpisania umowy.

---

#### 6. Gwarancja i wsparcie

- Wykonawca zapewni wsparcie w zakresie instalacji, aktywacji oraz przypisania licencji,
- Minimalny okres gwarancji i aktualizacji: zgodnie z modelem licencyjnym producenta.

## II. Zakup i wdrożenie systemu SIEM wraz z infrastrukturą sprzętową

---

### 1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

- dostawa i wdrożenie systemu klasy **SIEM (Security Information and Event Management)** umożliwiającego monitorowanie i analizę zdarzeń bezpieczeństwa w czasie rzeczywistym,
  - dostarczenie niezbędnej infrastruktury sprzętowej (serwer/appliance lub dedykowane urządzenie z systemem SIEM),
  - konfiguracja, integracja i uruchomienie systemu w środowisku Zamawiającego,
  - szkolenie administratorów systemu (minimum 1-dniowe).
- 

### 2. Cele realizacji zamówienia

Wdrożenie systemu SIEM ma na celu:

- zwiększenie poziomu bezpieczeństwa informatycznego w Urzędzie poprzez ciągły nadzór nad zdarzeniami systemowymi i sieciowymi,
  - zapewnienie detekcji incydentów bezpieczeństwa w czasie rzeczywistym,
  - integrację źródeł logów z różnych komponentów środowiska IT (serwery, zapory sieciowe, urządzenia końcowe, usługi sieciowe),
  - wsparcie w spełnieniu wymagań prawnych wynikających z KRI, Ustawy o KSC oraz przyszłej dyrektywy NIS2.
- 

### 3. Wymagania funkcjonalne systemu SIEM

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu.

6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
7. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie
8. System musi zapewniać retencję danych w okresie minimum 365 dni.
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
10. System musi umożliwiać rozbudowę bez potrzeby wyłączenia lub restartu środowiska.
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
14. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregośkolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
18. Interfejs musi posiadać angielską lub polską wersję językową.
19. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius

- 
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
  23. System musi wspierać mechanizm logowania typu Single Sign On.
  24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
  25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
  26. System powinien umożliwiać zarządzanie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
  27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
  28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
  29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
  30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
  31. System musi pozwalać na tworzenie parserów z poziomu GUI
  32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
  33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
  34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
  35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
  36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
  37. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

- 
- Syslog,
  - WEF,
  - Flat file,
  - Event log,
  - WMI,
  - SNMP trap,
  - XML,
  - JSON,
  - JDBC/ODBC
  - CSV,
  - Email,

38. Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

39. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.

40. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.

41. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.

42. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.

43. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.

44. System musi posiadać predefiniowany zestaw parserów zdarzeń.

45. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta

46. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.



47. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
48. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
49. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
50. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
51. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
52. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
53. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
54. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
55. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
56. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
57. Wykrycia dowolnej treści w logach,
58. Wykrycia wystąpienia wartości pola na wybranej liście,
59. Wykrycia niewystępowania wartości pola na wybranej liście,
60. Wykrycia zmiany jednego z kilku pól,
61. Wykrycia zdarzeń występujących z zadaną częstotliwością,
62. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
63. Wykrycia zaniku Wiadomości,
64. Wykrycia nowej wartości pola w zadanym okresie czasu,

- 
65. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
  66. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
  67. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
  68. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
  69. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
  70. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
  71. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
  72. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
  73. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
  74. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
  75. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
  76. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
  77. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
  78. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.

- 
79. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
  80. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
  81. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
  82. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
  83. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
  84. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres 3 lat.
  85. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
  86. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
  87. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
  88. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
  89. System musi umożliwiać integrację z Mitre ATT@CK.
  90. Reguły korelacyjne, alerty i obsługa incydentów
  91. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
  92. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
  93. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.

- 
94. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
95. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
96. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
97. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
98. Zamawiający wymaga wdrożenia systemu Security Information and Event Management (SIEM), który będzie zapewniał zaawansowane monitorowanie, analizę oraz korelację zdarzeń w infrastrukturze IT. System musi wspierać wykrywanie incydentów bezpieczeństwa oraz spełniać wymagania określone w aktualnych przepisach i normach dotyczących cyberbezpieczeństwa.
99. Wdrożenie systemu SIEM musi zostać zrealizowane przez:
- Wykwalifikowanego integratora posiadającego doświadczenie w implementacji i konfiguracji systemów SIEM oraz stosowne certyfikaty potwierdzające kompetencje w zakresie cyberbezpieczeństwa i administracji systemami IT.
  - Producenta oprogramowania SIEM, który zapewni pełne wsparcie w zakresie wdrożenia, integracji oraz dalszej eksploatacji systemu.

Oferowany system musi być wyposażony we wbudowany model językowy (LLM/GPT), dostarczony przez Producenta i stanowiący integralną część oferowanej platformy. Model językowy musi działać lokalnie w infrastrukturze Zamawiającego lub w środowisku chmurowym należącym do Producenta, z zapewnieniem zgodności z wymaganiami w zakresie bezpieczeństwa i ochrony danych obowiązującymi u Zamawiającego.

System musi umożliwiać integrację z zewnętrznymi modelami językowymi takimi jak OpenAI, Fireworks, lub modelem językowym (LLM) zgodnym ze standardem Ollama, z zachowaniem pełnej zgodności z zasadami bezpieczeństwa i ochrony danych obowiązującymi u Zamawiającego.

System musi umożliwiać definiowanie kontekstu organizacyjnego Zamawiającego, w tym: wykorzystywanych technologii, struktury organizacyjnej oraz obowiązujących wymagań prawnych. Na podstawie wprowadzonych danych wbudowany model językowy (LLM) ma zapewniać generowanie wyników analizy dostosowanych do specyfiki działalności Zamawiającego.

Wbudowany model językowy (LLM), stanowiący integralną część oferowanego systemu, musi umożliwiać dynamiczną analizę gromadzonych danych, w szczególności w zakresie:

- 
- automatycznego wyjaśnienia analizowanego zdarzenia,
  - weryfikacji potencjalnego naruszenia bezpieczeństwa wraz z rekomendacją działań naprawczych,
  - klasyfikacji wykrytego zagrożenia z wykorzystaniem matrycy MITRE ATT&CK,
  - opisu wektora ataku,
  - wykrycia naruszenia danych wrażliwych.

Oprogramowanie musi udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.

System musi umożliwiać rozbudowywanie funkcji Asystenta AI o nowe zapytania/prompty w kontekście analizy logów. Utworzone zapytania muszą być dostępne dla wszystkich użytkowników systemu za pomocą nowych przycisków lub pozycji list rozwijalnych.

Oprogramowanie powinno udostępniać funkcjonalność Asystenta sztucznej inteligencji, umożliwiającego – w oparciu o analizę wykrytych zagrożeń – automatyczne generowanie konfiguracji reguł korelacyjnych, które mogą zostać bezpośrednio zaimplementowane w oferowanej platformie.

Asystent AI musi pozwalać na budowanie odpowiedzi w dowolnym języku.

Asystent AI musi automatycznie dopasowywać zdarzenie do technik i taktów matrycy MITRE.

Asystent AI musi dokonywać automatycznej izolacji obiektów IoC ze wskazanego rekordu logów.

---

## 4. Wymagania sprzętowe i licencyjne

### 1. Infrastruktura sprzętowa:

- serwer lub appliance o parametrach zapewniających wydajność przetwarzania minimum 1000 EPS (Events Per Second), potwierdzoną przez producenta lub wykonawcę,
- procesor: minimum 8 rdzeni fizycznych (64-bitowy, klasy serwerowej),
- pamięć RAM: minimum 32 GB z możliwością rozbudowy do co najmniej 128 GB,
- macierz dyskowa lub zestaw dysków o łącznej pojemności minimum 4 TB przeznaczonej na przechowywanie logów, przy czym zaleca się rozdzielenie

przestrzeni systemowej (SSD) od przestrzeni przeznaczonej na dane (HDD/SSD klasy Enterprise),

- redundantne zasilanie (minimum dwa niezależne zasilacze),
- obsługa RAID co najmniej poziomów 0, 1, 5, 10,
- interfejsy sieciowe: minimum 2 porty 1 GbE (zalecane wsparcie dla 10 GbE),
- gwarancja: minimum 36 miesięcy, w formule on-site (naprawa w miejscu instalacji).

## 2. Licencja na system SIEM:

- licencja wieczysta lub czasowa (minimum 3 lata),
  - brak ograniczeń ilości logowanych urządzeń lub możliwość obsługi minimum 50 źródeł logów.
- 

## 5. Integracja i uruchomienie

Wykonawca zobowiązany jest do:

- instalacji, konfiguracji i uruchomienia systemu SIEM w środowisku Zamawiającego,
  - integracji co najmniej z: Active Directory, firewall, serwery Windows, logi z systemu antywirusowego oraz stacji roboczych,
  - przeprowadzenia testów poprawności działania,
  - przekazania dokumentacji technicznej (schematy, opisy konfiguracji, instrukcja obsługi).
- 

## 6. Szkolenie

Wykonawca przeprowadzi szkolenie dla min. 2 administratorów (szkolenie online lub stacjonarne):

- zakres: obsługa, analiza incydentów, tworzenie reguł i raportów,
  - czas trwania: minimum 6 godzin dydaktycznych,
  - zakończone wydaniem zaświadczenia lub certyfikatu.
-

## 7. Wsparcie techniczne i gwarancja

- Gwarancja na wdrożone rozwiązanie: minimum 36 miesięcy,
  - Wsparcie techniczne (helpdesk): w dni robocze 8:00–16:00,
  - Wsparcie producenta systemu SIEM w wymiarze 32 roboczogodzin do wykorzystania w okresie 36 miesięcy od dnia podpisania protokołu odbioru końcowego.
  - Czas reakcji na zgłoszenie: do 8 godzin roboczych.
- 

## 8. Termin realizacji

Zamówienie musi być zrealizowane w ciągu **45 dni kalendarzowych** od dnia podpisania umowy.

### **III. Zakup i wdrożenie systemu backupu danych serwerów i stacji roboczych Urzędu**

---

#### **1. Przedmiot zamówienia**

Przedmiotem zamówienia jest:

- zakup licencjonowanego oprogramowania do backupu serwerów fizycznych, maszyn wirtualnych oraz stacji roboczych,
  - dostarczenie niezbędnych licencji i/lub komponentów sprzętowych (jeśli wymagane przez producenta),
  - wdrożenie kompletnego, zautomatyzowanego i centralnie zarządzanego systemu wykonywania kopii zapasowych,
  - konfiguracja systemu zgodnie z wymaganiami Zamawiającego,
  - przeszkolenie wskazanych pracowników.
- 

#### **2. Cel realizacji zamówienia**

Celem wdrożenia systemu backupu jest:

- zapewnienie ciągłości działania systemów informatycznych Urzędu,
  - zabezpieczenie kluczowych danych i plików przed skutkami awarii, cyberataków, błędów użytkownika lub zasyfrowania (np. ransomware),
  - umożliwienie odzyskania danych na poziomie całych maszyn wirtualnych, fizycznych serwerów, wybranych woluminów, baz danych lub pojedynczych plików,
  - zapewnienie zgodności z obowiązującymi standardami KRI i rekomendacjami w zakresie bezpieczeństwa danych.
- 

#### **3. Zarządzanie i magazyny**

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
  - a. Obudowa rack rozmiar: 1U
  - b. Procesor: min. 8 rdzeni, 16 wątków, min. taktowanie 2.6GHz

- 
- c. Pamięć RAM: 16GB
  - d. Przestrzeń dostępna na przechowywanie danych:  
Min. 14TB po RAID 5
  - e. Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
  - f. Redundantne zasilanie,
  - g. Interfejsy sieciowe: Min. 2szt. Ethernet 1Gb
  - h. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.
4. Produkt dostępny w polskiej wersji językowej.
  5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
  6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
  7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
  8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
  9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
  10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
  11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
  12. System zarządzania nie może być oparty o relacyjne bazy danych.
  13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
  14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
  15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
  16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
  17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
  18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
  19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem

stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.

20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.

- 
34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
  35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
  36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
  37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
  38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
  39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
  40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
  41. System musi pozwalać na automatyczne aktualizacje oprogramowania.
  42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
  43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
  44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
  45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
  46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
  47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
  48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.

49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u
57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny
58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
60. Możliwość generowania raportów dobowych w oparciu o harmonogram
61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.

---

64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

---

#### 4. Wspierane systemy

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

- Alpine 3.10+,
- Debian: 9+,
- Ubuntu: 16.04+,
- Fedora: 29+,
- CentOS: 7+,
- RHEL: 6+,
- openSUSE: 15+,
- SUSE Enterprise Linux(SLES): 12 SP2+,
- macOS: 10.13+,
- Windows: 7, 8.1, 10(1607+),
- Windows Server: 2008 R2+,

Środowisk wirtualnych:

- Hyper-V 2016+,
- VMware: 6.7+.

---

#### 5. Środowiska fizyczne i bazy danych

- Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
- Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
- Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
- Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
- System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.

- 
- System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych.
  - System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
  - W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
  - Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
  - Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
  - Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
  - Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
  - Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
  - Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).
- 

## 6. Środowiska wirtualne

1. System musi posiadać wsparcie dla wirtualizatorów VMware vSphere, Microsoft Hyper-V oraz Proxmox Virtual Environment

2. Dla wspieranych wirtualizatorów system musi posiadać możliwość zabezpieczania całych maszyn wirtualnych bez konieczności instalacji agentów backupowych wewnątrz maszyn wirtualnych
  3. Dla wspieranych środowisk wirtualnych system musi umożliwiać wykonanie kopii pełnej, różnicowej oraz przyrostowej, a dodatkowo umożliwiać wykonanie procesu deduplikacji
  4. System musi wspierać kopię w trybie application-aware dla wirtualizatorów Hyper-V oraz vSphere.
  5. Dla środowiska VMware, system musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
  6. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
  7. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
  8. Dla wybranych wirtualizatorów, system kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
  9. Rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
  10. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku dla wybranych wirtualizatorów.
- 

## 7. Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)

3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

---

## 8. Anty-ransomware i bezpieczeństwo

1. System plików rozwiązywania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

---

## 9. Licencjonowanie i wsparcie techniczne

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.

- 
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
  3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
  4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
  5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
  6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymaniu infrastruktury Zamawiającego.
  7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.
  8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
  9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
  10. Wsparcie techniczne producenta musi zostać dostarczone na min. 36 miesięcy.
  11. Licencje powinny umożliwiać replikacje na własne zasoby.
  12. W ramach utrzymania ciągłości wsparcia technicznego przez min. 60 miesięcy u producenta dostarczanego rozwiązania, producent jest zobowiązany do wymiany dostarczanej warstwy sprzętowej w momencie kiedy zamawiający zdecyduje się na kontynuację wsparcia technicznego na kolejne min. 36 miesięcy.
- 

## 10. Termin realizacji i wdrożenie

- Wdrożenie musi zostać realizowane bezpośrednio przez producenta oferowanego systemu backupowego w formie zdalnej.
- Wdrożenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu backupowego.
- Wdrożenie musi zakończyć się dostarczeniem dokumentacji powdrożeniowej, przygotowanej przez dedykowanego inżyniera od producenta systemu backupowego.
- Pomoc wdrożeniowa powinna trwać nie mniej niż 2h w ustalonym terminie przez zamawiającego.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

- 
- Szkolenie zostanie przeprowadzone w formie zdalnej lub stacjonarnej dla minimum dwóch pracowników Zamawiającego w wymiarze co najmniej 4 godzin.
  - Wdrożenie kompletnego rozwiązania backupowego musi zostać zrealizowane w ciągu **30 dni kalendarzowych** od dnia podpisania umowy.