

Numer postępowania: **MAE/636/2023,**

Postępowanie pn.: „**Wdrożenie i świadczenie usługi monitoringu bezpieczeństwa teleinformatycznego SOC, utrzymanie systemu kopii zapasowych, dostarczenie i wdrożenie systemu wirtualizacji oraz dostarczenie i wdrożenie UTM**”

Szczegółowy opis przedmiotu zamówienia

1 Przedmiot zamówienia.

1.1 Przedmiotem postępowania są:

- 1.1.1 wdrożenie i świadczenie usługi monitoringu bezpieczeństwa teleinformatycznego SOC (Security Operations Center). Szczegółowe wymagania opisane są w pkt. 2.
- 1.1.2 wdrożenie i utrzymanie systemu kopii zapasowych. Szczegółowe wymagania opisane są w pkt. 3.
- 1.1.3 dostarczenie i wdrożenie systemu wirtualizacji. Szczegółowe wymagania opisane są w pkt. 4.
- 1.1.4 dostarczenie i wdrożenie systemu klasy UTM. Szczegółowe wymagania opisane są w pkt. 5. w celu podniesienia poziomu bezpieczeństwa teleinformatycznego Zamawiającego.

2 Parametry techniczne i wymagania minimalne dotyczące wdrożenia i świadczenia usługi monitoringu bezpieczeństwa SOC.

2.1 Wymagania ogólne.

- 2.1.1 Usługa monitoringu bezpieczeństwa teleinformatycznego SOC (Security Operations Center) ma na celu identyfikację zagrożeń i incydentów bezpieczeństwa w systemach teleinformatycznych Zamawiającego.
- 2.1.2 Usługa świadczona jest na systemie monitoringu SIEM (Security Information and Event Management), dostarczonym przez Wykonawcę.
- 2.1.3 W celu detekcji zagrożeń i incydentów system SIEM agreguje, normalizuje, koreluje i analizuje logi przesyłane przez monitorowane systemy źródłowe. Na podstawie wyników działania zdefiniowanych reguł korelacyjnych, system generuje alarmy o różnym poziomie krytyczności. Klasyfikacja incydentów Zamawiającego zakłada 4 poziomy krytyczności incydentów: krytyczny, wysoki, średni, niski/informacyjny.
- 2.1.4 W ramach usługi SOC, Wykonawca monitoruje w trybie ciągłym 24/7 poziom bezpieczeństwa infrastruktury Zamawiającego zgodnie z uzgodnionymi z Zamawiającym scenariuszami monitoringu, weryfikuje podnoszone przez system SIEM alarmy i w przypadku potwierdzenia anomalii dokonuje klasyfikacji incydentu, a następnie stosownie do poziomu krytyczności incydentu podejmuje działania uzgodnione z Zamawiającym w scenariuszu reakcji. Szczegółowa klasyfikacja incydentów będzie uzgodniona z Zamawiającym według kryteriów ustalonych na etapie analizy przedwdrożeniowej.
- 2.1.5 W trakcie świadczenia usługi SOC Wykonawca ściśle współpracuje z Zamawiającym w obszarze mitygacji incydentów, usuwania przyczyn ich powstania i skutków.

2.2 Wymagania w zakresie modelu funkcjonowania zespołu SOC.

- 2.2.1 Wykonawca zapewni ciągłość monitorowania i obsługi incydentów przez SOC w trybie 24/7/365.
- 2.2.2 Wykonawca zapewni możliwość rejestracji zgłoszenia podejrzenia incydentu lub problemu związanego z realizacją usługi SOC poprzez udostępniony przez niego system zgłoszeń lub za pośrednictwem zgłoszenia mailowego.
- 2.2.3 Zespół SOC prowadzi rejestr zgłoszeń i incydentów.
- 2.2.4 Zespół SOC rozwiązuje incydenty bezpieczeństwa zgodnie warunkami SLA:

Klasyfikacja incydentu	Czas podjęcia	Czas reakcji (minimum wstępna analiza i rekomendacja działań)
Krytyczny	15 min.	2 godz.
Wysoki	1 godz.	4 godz.
Średni	4 godz.	12 godz.
Niski/Informacyjny	12 godz.	24 godz.

- 2.2.5 Raportowanie w ramach usługi SOC jest realizowane w następujących cyklach:
 - 2.2.5.1 raport o incydencie krytycznym lub wysokim każdorazowo w przypadku jego wystąpienia;
 - 2.2.5.2 raporty z podsumowaniem zarejestrowanych i podjętych incydentów w cyklu miesięcznym.
- 2.2.6 Wykonawca zobowiązany jest do gromadzenia informacji o wszelkich zarejestrowanych w systemie SIEM incydentach bezpieczeństwa dla świadczonej usługi SOC oraz niezwłocznego przekazywania Zamawiającemu informacji o incydentach bezpieczeństwa.
- 2.2.7 Wykonawca świadczy usługę SOC z własnego centrum operacji bezpieczeństwa zlokalizowanego w Polsce.
- 2.2.8 Komunikacja z zespołem SOC odbywa się w języku polskim.

- 2.2.9 W związku z pojawiającymi się nowymi zagrożeniami i wymaganiami w obszarze cyberbezpieczeństwa (podatności, ataki, przepisy prawa, zalecenia) Wykonawca zapewnia propozycje nowych i modyfikacji scenariuszy monitoringu i scenariuszy reakcji.

2.3 Zakres wdrożenia usługi SOC.

- 2.3.1 Wykonawca przeprowadzi analizę przedwdrożeniową, mającą na celu identyfikację źródłowych systemów, które zostaną objęte monitoringiem. Maksymalna liczba monitorowanych systemów źródłowych wynosi 5.
- 2.3.2 Wykonawca opracuje i wdroży do 10 scenariuszy monitoringu odpowiadające potrzebom Zamawiającego w zakresie bezpieczeństwa teleinformatycznego. Implementacja inicjalnych scenariuszy bezpieczeństwa zostanie przeprowadzona według zaleceń Wykonawcy. Zamawiający zastrzega sobie możliwość zlecenia dostosowania lub zmiany scenariuszy w trakcie trwania świadczenia usługi SOC po uprzednim uzgodnieniu z Wykonawcą.
- 2.3.3 Wykonawca opracuje we współpracy z Zamawiającym scenariusze reakcji oraz szczegółową klasyfikację incydentów.
- 2.3.4 Wykonawca dostarczy dokumentację powdrożeniową, opisującą zakres i sposób realizacji usługi SOC.
- 2.3.5 Wykonawca zapewni obsługę incydentów zgodnie ze scenariuszami reakcji oraz gwarantowanymi parametrami SLA.
- 2.3.6 Okres świadczenia usługi SOC wynosi 24 miesiące od daty wdrożenia.
- 2.3.7 Wykonawca zapewni aktualność oprogramowania systemu SIEM przez cały okres świadczenia usługi SOC.
- 2.3.8 Finalne strojenie i stabilizacja systemu SIEM zostanie przeprowadzona w terminie do 30 dni od wdrożenia i wchodzi w zakres świadczenia usługi SOC
- 2.3.9 Wykonawca zapewni retencję gromadzonych danych zdarzeń do 30 dni (tzw. warm logs) oraz archiwizację gromadzonych danych zdarzeń do 12 miesięcy (tzw. cold logs).

2.4 Wymagania dot. systemu SIEM stosowanego na potrzeby realizacji usługi SOC.

- 2.4.1 Wykonawca zapewnia utrzymanie ciągłości działania systemu SIEM:
- 2.4.1.1 zapewnienie utrzymania nieprzerwanego, bezawaryjnego funkcjonowania systemu;
 - 2.4.1.2 świadczenie usług wsparcia technicznego poprzez przyjmowanie i diagnozę błędów;
 - 2.4.1.3 usuwanie awarii systemu wynikających z błędnego lub wadliwego, niezgodnego z dokumentacją działania systemu;
 - 2.4.1.4 zapewnienie odpowiedniego poziomu bezpieczeństwa systemu, usuwanie podatności, wdrażanie poprawek bezpieczeństwa;
 - 2.4.1.5 świadczenie pomocy technicznej w języku polskim;
- 2.4.2 Wymagana minimalna dostępność systemu SIEM w ujęciu miesięcznym wynosi 98%.
- 2.4.3 Czas usunięcia awarii (niedostępność lub brak dostępu do systemu SIEM) – do 48 godzin.
- 2.4.4 Wykonawca zapewni utrzymanie i obsługę systemu SIEM przez zespół SOC przez cały okres świadczenia usługi SOC.
- 2.4.5 Na potrzeby wglądu oraz weryfikacji funkcjonowania rozwiązania Wykonawca zapewni Zamawiającemu bezpieczny dostęp poprzez VPN do systemu SIEM, do gromadzonych danych oraz do raportów i dashboardów.
- 2.4.6 Wykorzystywany system SIEM musi być dojrzałym, uznanym na rynku produktem. Jako potwierdzenie spełnienia wymagania uznane będzie:
- 2.4.6.1 zakwalifikowanie oferowanego systemu SIEM w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM (w raportach najbardziej aktualnych na dzień składania ofert) lub
 - 2.4.6.2 zakwalifikowanie oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms (w raportach najbardziej aktualnych na dzień składania ofert).
- 2.4.7 Zamawiający nie dopuszcza stosowania przez Wykonawcę systemu SIEM typu open-source.
- 2.4.8 System SIEM powinien posiadać certyfikację Common Criteria for IT Security Evaluation (commoncriteriaportal.org) na poziomie nie niższym niż EAL3 lub równoważną.
- 2.4.9 System SIEM musi być w sprzedaży na rynku co najmniej 3 lata na rynku polskim oraz posiadać wsparcie techniczne producenta oraz aktualizacje przez cały okres świadczenia usługi SOC.
- 2.4.10 System SIEM musi mieć możliwość pracy w architekturze pozwalającej na instalację i konfigurację w wielu lokalizacjach.
- 2.4.11 System SIEM musi mieć możliwość pracy w architekturze wysokiej dostępności (HA).
- 2.4.12 System SIEM musi umożliwiać monitoring aktywności w sieci i na urządzeniach w czasie rzeczywistym.
- 2.4.13 System SIEM powinien automatycznie generować powiadomienia alarmowe w odpowiedzi na wykryte anomalie bezpieczeństwa.
- 2.4.14 System SIEM powinien wspierać integrację z różnymi systemami bezpieczeństwa.
- 2.4.15 Kolektory danych, zbierające logi z infrastruktury Zamawiającego, będą zainstalowane przez Wykonawcę na zasobach serwerowych Wykonawcy. Kolektory będą zbierać dane ze źródeł stanowiących systemy zabezpieczeń i systemy uwierzytelniania Zamawiającego (tj. NGFW, IPS, IDS, AV, EDR, AD, NAC, PAM, IAM, SKD itp.), a także z serwerów i stacji roboczych, i przekazywać je do korelacji i analizy do modułu analitycznego

- SIEM. Liczba kolektorów danych zostanie określona w trakcie analizy przedwdrożeniowej przeprowadzonej przez Wykonawcę.
- 2.4.16 System SIEM musi umożliwiać zainstalowanie i komunikację z dowolną liczbą dedykowanych kolektorów danych, które umożliwiają zbieranie (kolekcję) logów w wydzielonych segmentach infrastruktury i dalsze ich transferowanie do systemu centralnego w celu analizy.
 - 2.4.17 System SIEM powinien umożliwiać niezależną analizę zdarzeń dla wskazanych oddzielonych segmentach infrastruktury przy zachowaniu swobody wykorzystania wspólnej puli zalicencjonowanych komponentów.
 - 2.4.18 System SIEM nie może ograniczać zakresu informacji pochodzących z monitorowanych systemów, które są niezbędne do korelowania zdarzeń w czasie rzeczywistym. W szczególności system SIEM nie może ograniczać liczby przetwarzanych zdarzeń w jednostce czasu w zakresie rejestrowanych zdarzeń (np. EPS - events per second, FPM – flows per minute, itp), ani ograniczać ilości danych przetwarzanych w systemie na podstawie dostarczanych zdarzeń w jednostce czasu w zakresie rejestrowanych zdarzeń (np. GB per day, itp).
 - 2.4.19 System SIEM musi mieć wbudowany framework Mitre Att&ck i pokrywać ponad 120 technik z macierzy TTP.
 - 2.4.20 System SIEM powinien być dostarczony w wersji umożliwiającej uruchomienie funkcjonalności SOAR (Security Orchestration, Automation and Response) dla co najmniej jednego użytkownika.
 - 2.4.21 Wszystkie komponenty dostarczonego oprogramowania, w tym SIEM i SOAR, powinny być natywnie zintegrowane i wspierane przez producenta w całym okresie realizacji umowy.
 - 2.4.22 Licencjonowanie komponentu SOAR nie może ograniczać liczby kont indywidualnych użytkowników systemu (tzw. named accounts).
 - 2.4.23 System SIEM powinien umożliwiać taki sposób zapisu i przechowywania danych, który nie wymaga dedykowanej strukturyzowanej bazy danych i pozwala na przechowywanie danych na dowolnym nośniku w postaci tzw. plików płaskich.
 - 2.4.24 System SIEM powinien umożliwiać współpracę z natywnym agentem instalowanym na monitorowanej stacji końcowej (stacja robocza lub serwer), który zapewnia rozszerzenie zakresu monitorowania parametrów ponad te zawarte w standardowych logach.
 - 2.4.25 Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie.
 - 2.4.26 System SIEM musi dysponować opcjonalną funkcjonalnością analizy zachowań użytkowników i urządzeń (tzw. user and entity behavior analytics, UEBA), wykorzystującą metody uczenia maszynowego do wykrywania anomalii.
 - 2.4.27 Centralny moduł analityczny SIEM jest hostowany w chmurze lub środowisku serwerowym Wykonawcy.
 - 2.4.28 Centralny moduł analityczny SIEM udostępnia zaawansowane funkcje raportowania, umożliwiające generowanie szczegółowych raportów dotyczących różnych aspektów bezpieczeństwa infrastruktury informatycznej.
 - 2.4.29 System powinien umożliwiać zbieranie, normalizację i korelację logów z różnych źródeł w jednolitym formacie.
 - 2.4.30 System SIEM powinien być zainstalowany na środowisku serwerowym Wykonawcy, zlokalizowanym w centrum przetwarzania danych o standardzie min. EN 50600-1:2019, które posiada właściwą ochronę elektromagnetyczną. Potwierdzeniem zastosowania ochrony jest Certyfikat Ochrony Elektromagnetycznej (Ustawa o ochronie informacji niejawnych, art. 50, ust. 5) wystawiony przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego.
 - 2.4.31 System SIEM musi umożliwiać pobieranie logów co najmniej następującymi protokołami:
 - 2.4.31.1 syslog UDP/TCP;
 - 2.4.31.2 SNMP;
 - 2.4.31.3 WMI;
 - 2.4.31.4 logi i informacje przechowywane w bazach danych (Oracle, MS SQL, MySQL, PostgreSQL);
 - 2.4.31.5 pliki tekstowe;
 - 2.4.31.6 logi JMS, JMX;
 - 2.4.31.7 dane z systemów wirtualizacji;
 - 2.4.31.8 dane z systemów chmurowych;
 - 2.4.31.9 NetFlow v5 i v9, sFlow, jFlow;
 - 2.4.31.10 zbiory wskazane w katalogach.
 - 2.4.32 System SIEM musi umożliwiać pobieranie logów/zdarzeń co najmniej z następujących systemów i aplikacji:
 - 2.4.32.1 systemy Windows 2012/2016/2019/2022 oraz /7/8.x/10/11;
 - 2.4.32.2 systemy Linux (każda dystrybucja);
 - 2.4.32.3 urządzenia sieciowe Cisco, Nortel, Alcatel, MikroTik, Juniper, Fortinet, Dell, Extreme networks, Watchguard, Aruba, HPE.

Przez pozyskiwanie logów rozumie się: pobranie logów i zapisanie w bazie systemu SIEM, klasyfikacja zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.), normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source_ip itp.
 - 2.4.33 System SIEM musi umożliwiać parsowanie logów o długości 10 000 znaków oraz zawierających więcej niż jedną linię.

2.5 Inne wymagania względem Wykonawcy

- 2.5.1 Zamawiający wymaga, aby usługa SOC była realizowana zgodnie z prawem polskim, w szczególności z Ustawą o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 z późn. zm.).
- 2.5.2 Wykonawca spełnia wymagania opisane w Rozporządzeniu Ministra Cyfryzacji z 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwa (Dz.U. 2019 poz. 2479)
- 2.5.3 Wykonawca musi posiadać wdrożone i funkcjonujące normy lub ich odpowiedniki w polskim lub europejskim układzie normalizacyjnym:
 - 2.5.3.1 PN-EN ISO/IEC 27001 lub równoważną dotyczącą zarządzania bezpieczeństwem informacji;
 - 2.5.3.2 PN-EN ISO 22301 lub równoważną dotyczącą zarządzania ciągłością działania;
 - 2.5.3.3 ISO/IEC 27017 lub równoważną dotyczącą bezpieczeństwa informacji w chmurze obliczeniowej;
 - 2.5.3.4 ISO/IEC 27018 lub równoważną dotyczącą dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.

3 Parametry techniczne i wymagania minimalne dotyczące wdrożenia i utrzymania systemu kopii zapasowych.

3.1 Wymagania ogólne.

- 3.1.1 Wykonawca jest odpowiedzialny za zaprojektowanie, dostawę licencji i wdrożenie Oprogramowania standardowego ściśle dostosowanego jakościowo i ilościowo do wymagań.
- 3.1.2 Oprogramowanie standardowe dostarczane przez Wykonawcę będzie dostarczone, skonfigurowane i wdrożone „pod klucz”. Wdrożenie obejmie co najmniej następujące czynności:
 - 3.1.2.1 Opracowanie polityki backupu z uwzględnieniem oczekiwań w zakresie RPO & RTO, zawierającej, m.in.:
 - 3.1.2.1.1 Retencja backupu i GFS;
 - 3.1.2.1.2 Metoda i granularność zadań backupu i odtwarzania;
 - 3.1.2.1.3 Harmonogram zadań backupu;
 - 3.1.2.1.4 Rekomendacje w zakresie integracji zadań z systemami operacyjnymi i aplikacjami;
 - 3.1.2.1.5 Schemat powiadomień dla poszczególnych zadań.
 - 3.1.2.2 Wdrożenie systemu kopii zapasowych wraz z konfiguracją zadań backupu zgodnie z opracowaną polityką backupu.
 - 3.1.2.3 Wykonanie odtworzeń testowych w infrastrukturze backupu.
 - 3.1.2.4 Instruktaż stanowiskowy 4 godziny.
- 3.1.3 Wykonawca przygotuje dokumentację powykonawczą wdrażanego Oprogramowania.
- 3.1.4 W całym okresie związania umową Wykonawca zapewni wsparcie techniczne dotyczące systemu kopii zapasowych o następujących parametrach:
 - 3.1.4.1 Dostępność wsparcia w dni robocze (od poniedziałku do piątku) od 8:00 do 16:00 z wyłączeniem dni ustawowo wolnych od pracy;
 - 3.1.4.2 Podjęcie się obsługi zleceń serwisowych lub zleceń wsparcia technicznego najdalej w następnym dniu roboczym od zgłoszenia;
 - 3.1.4.3 Zagwarantowanie min 6 godzin miesięcznie na obsługę zleceń Zamawiającego.

3.2 System kopii zapasowej

- 3.2.1 Zamawiający oczekuje dostarczenia jednego, kompletnego systemu kopii zapasowych, spełniającego wszystkie poniższe wymagania. Nie dopuszcza się dostarczenia dwóch odrębnych, wymagających integracji rozwiązań.
- 3.2.2 Zamawiający wymaga, by dostarczone licencje umożliwiały wykonywanie kopii zapasowych, co najmniej:
 - 3.2.2.1 4 maszyn wirtualnych,
 - 3.2.2.2 1 serwera fizycznego,
 - 3.2.2.3 15 stacji roboczych.
- 3.2.3 Dostarczany system musi zapewniać możliwość automatycznego wykonywania wyniesionej kopii zapasowej danych, co oznacza przesyłanie i składowanie kopii poza siedzibą Zamawiającego, w okresie nie krótszym niż 24 miesiące od daty wdrożenia.
- 3.2.4 W celu realizacji automatycznego wykonywania wyniesionej kopii zapasowej danych, Zamawiający wymaga udostępnienia:
 - 3.2.4.1 infrastruktury udostępniającej przestrzeń dyskową na składowanie kopii zapasowych w centrum przetwarzania danych spełniającym, co najmniej następujące wymagania:
 - 3.2.4.1.1 musi posiadać aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;
 - 3.2.4.1.2 musi posiadać redundantne wewnętrzne linie dystrybucji energii elektrycznej obsługujące macierze dyskowe;
 - 3.2.4.1.3 musi posiadać redundantne wewnętrzne linie chłodu równoległe obsługujące macierze dyskowe;
 - 3.2.4.1.4 musi posiadać możliwość, odłączania każdego elementu linii dystrybucji energii elektrycznej i chłodu w celu poddania czynności serwisowej, tak aby nie zakłócić normalnej pracy urządzeń dwuzasilaczowych;

- 3.2.4.1.5 musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
- 3.2.4.1.6 musi posiadać całodobową ochronę fizyczną z rejestracją kamer monitoringu wizyjnego na zewnątrz i wewnątrz budynku;
- 3.2.4.1.7 musi być zlokalizowane na terenie Polski;
- 3.2.4.1.8 musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenie ze sprzętem IT muszą być wyposażone w zautomatyzowaną aparaturę gaśniczą;
- 3.2.4.1.9 musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatu prądotwórczego;
- 3.2.4.1.10 musi posiadać UPS'y pracujące w nadmiarowej konfiguracji (co najmniej N+1), zapewniając nieprzerwane zasilanie macierzy dyskowej;
- 3.2.4.1.11 musi pozwalać, aby dystrybucja energii elektrycznej do macierzy dyskowej odbywała się z wykorzystaniem minimum dwóch niezależnych torów zasilania, z minimum jednym torem gwarantowanym (podtrzymanie zasilania z wykorzystaniem UPS i agregatu prądotwórczego);
- 3.2.4.1.12 musi posiadać Certyfikat Ochrony Elektromagnetycznej wydany przez Agencję Bezpieczeństwa Wewnętrznego;
- 3.2.4.1.13 musi spełniać standardy normy EN 50600-1:2019 (dostępność: klasa dostępności 3 lub 4, bezpieczeństwo fizyczne: klasa ochrony 3 lub 4, efektywność energetyczna: poziom szczegółowości 3 lub 4);
- 3.2.4.2 przestrzeni dyskowej na składowanie kopii zapasowej o wielkości 30 TB z możliwością zwiększenia do co najmniej 100 TB (zwiększenie pojemności powyżej 30 TB nie jest elementem oferty i nie podlega wycenie), w oparciu o wysokodostępną macierz dyskową spełniającą poniższe wymagania:
 - 3.2.4.2.1 macierz musi pozwalać na tworzenia kopii zapasowych z wykorzystaniem transmisji wielostrumieniowej;
 - 3.2.4.2.2 macierz musi posiadać redundancję wszystkich komponentów – brak pojedynczego punktu awarii. W przypadku awarii kontrolera, automatyczne przełączanie wystawianych zasobów na inny kontroler, którego wydajność jest nie mniejsza niż tego, który uległ awarii;
 - 3.2.4.2.3 macierz musi posiadać możliwość rozbudowy w trakcie jej pracy (online);
 - 3.2.4.2.4 rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, półka dyskowa, kontroler, zasilacz;
 - 3.2.4.2.5 macierz musi posiadać możliwość aktualizacji firmware trybie online, bez zauważalnego zanikania ścieżek dostępu do zasobów dyskowych macierzy;
- 3.2.4.3 łączy internetowe symetryczne o przepustowości nie mniejszej niż 1 Gb/s do infrastruktury, na której składowane będą wyniesione kopie zapasowe. Wykonawca nie zapewnia łączy po stronie Zamawiającego;
- 3.2.4.4 Zamawiający wymaga, aby Wykonawca w zakresie świadczonych usług chmurowych posiadał wdrożone i funkcjonujące normy lub ich odpowiedniki w polskim lub europejskim układzie normalizacyjnym:
 - 3.2.4.4.1 PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji,
 - 3.2.4.4.2 PN-EN ISO 22301 dotyczące zarządzania ciągłością działania,
 - 3.2.4.4.3 ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej,
- 3.2.5 Komunikacja pomiędzy Zamawiającym, a miejscem składowania danych wyniesionych musi odbywać się z wykorzystaniem bezpiecznego połączenia (co najmniej SSL lub IPSec).
- 3.2.6 Zamawiający wymaga, aby system przechowywania wyniesionych kopii zapasowych po stronie Wykonawcy nie umożliwiał przesłania niezasyfrowanej kopii zapasowej do wyniesionego miejsca składowania danych.
- 3.2.7 Zamawiający może zażądać wskazania dokładnej lokalizacji fizycznej urządzeń przetwarzania i składowania danych (z dokładnością do adresu i szafy w centrum przetwarzania danych).
- 3.2.8 Wykonawca zapewni samoobsługowy panel usługi systemu kopii wyniesionych, który posiada co najmniej poniższe funkcjonalności:
 - 3.2.8.1 zdalne monitorowanie i zarządzanie kopiami zapasowymi za pomocą jednego internetowego interfejsu użytkownika.
 - 3.2.8.2 zabezpieczenie dostępu do panelu usługi z wykorzystaniem protokołu SSL oraz dwuskładnikowego uwierzytelniania MFA (użytkownik, hasło i token);
 - 3.2.8.3 prezentacja stanu realizowanych oraz historycznych zadań backupu oraz możliwość eksportowania tych danych do pliku tekstowego;
 - 3.2.8.4 możliwość uruchamiania, zatrzymywania, powtarzania, włączania i wyłączania zadań backupu oraz pobierania rejestru zdarzeń;
 - 3.2.8.5 obsługa alarmów dotyczących zadań backupowych oraz stanu systemu oraz eksportowania ich do pliku tekstowego
 - 3.2.8.6 raportowanie i rozliczenia zapewniające pełny wgląd w czasie rzeczywistym w zasoby zaangażowane do przechowywania kopii zapasowych:
 - 3.2.8.6.1 możliwość przeglądania raportów;
 - 3.2.8.6.2 sprawdzanie poziomu wykorzystania przydzielonej bezpiecznej przestrzeni dyskowej;
 - 3.2.8.6.3 wyświetlanie statystyki dotyczącej liczby serwerów, stacji roboczych i wirtualnych maszyn obsługiwanych przez system.

- 3.2.9 Oprogramowanie systemu kopii zapasowej musi spełniać, co najmniej wymagania przedstawione poniżej:
- 3.2.9.1 Dostarczane licencje muszą zapewniać obsługę kopii zapasowych obciążeń określonych w pkt 3.2.2 oraz zawierać wsparcie producenta na minimum 1 rok.
 - 3.2.9.2 Wykonawca zapewni licencje systemu operacyjnego wymaganego do uruchomienia systemu kopii zapasowych ze wsparciem producenta w całym okresie związania umową.
 - 3.2.9.3 Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk produkcyjnych. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions>
 - 3.2.9.4 Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 i 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
 - 3.2.9.5 Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
 - 3.2.9.6 Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
 - 3.2.9.7 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.
 - 3.2.9.8 Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
 - 3.2.9.9 Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania, dla których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków.
 - 3.2.9.10 Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental).
 - 3.2.9.11 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.
 - 3.2.9.12 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.
 - 3.2.9.13 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 do takiej puli.
 - 3.2.9.14 Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
 - 3.2.9.15 Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania migawki (snapshota).
 - 3.2.9.16 Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
 - 3.2.9.17 Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
 - 3.2.9.18 Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
 - 3.2.9.19 Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
 - 3.2.9.20 Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
 - 3.2.9.21 Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie były przekraczane skonfigurowane przez administratora backupu poziomy opóźnień (latencji). Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
 - 3.2.9.22 Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
 - 3.2.9.23 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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.

- 3.2.9.24 Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
- 3.2.9.25 Oprogramowanie musi posiadać wsparcie dla NDMP.
- 3.2.9.26 Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
- 3.2.9.27 Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- 3.2.9.28 Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- 3.2.9.29 Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- 3.2.9.30 Repozytoria oparte o XFS muszą pozwalać na niezmiennosc danych przez określoną ilość czasu (tzw. Immutability)
- 3.2.9.31 Oprogramowanie musi mieć możliwość przesyłania backupów z wykorzystaniem wbudowanej akceleracji WAN dla łącz internetowych o niskiej przepustowości.
- 3.2.9.32 Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
- 3.2.9.33 Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- 3.2.9.34 Oprogramowanie musi umożliwić odtworzenie plików na maszynie operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- 3.2.9.35 Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- 3.2.9.36 Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
 - 3.2.9.36.1 Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
 - 3.2.9.36.2 BSD: UFS, UFS2
 - 3.2.9.36.3 Solaris: ZFS, UFS
 - 3.2.9.36.4 Mac: HFS, HFS+
 - 3.2.9.36.5 Windows: NTFS, FAT, FAT32, ReFS
 - 3.2.9.36.6 Novell OES: NSS
- 3.2.9.37 Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- 3.2.9.38 Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- 3.2.9.39 Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
- 3.2.9.40 Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
- 3.2.9.41 Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
- 3.2.9.42 Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych.
- 3.2.9.43 Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
- 3.2.9.44 Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych.
- 3.2.9.45 Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
- 3.2.9.46 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.
- 3.2.9.47 Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
- 3.2.9.48 Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
- 3.2.9.49 Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA.
- 3.2.9.50 Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
- 3.2.9.51 Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- 3.2.9.52 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.
- 3.2.9.53 Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych.

- 3.2.9.54 Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
- 3.2.9.55 Zamawiający nie wyraża zgody na zaoferowanie oprogramowania o otwartym kodzie źródłowym. Pod pojęciem oprogramowania z otwartym kod źródłowym Zamawiający rozumie oprogramowanie, którego kod źródłowy jest publicznie dostępny.

4 Parametry techniczne i wymagania minimalne dotyczące wdrożenia i utrzymania systemu wirtualizacji.

4.1 System wirtualizacji zgodny z „Vmware essential plus v8.0” lub równoważny.

- 4.1.1 Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
- 4.1.2 Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- 4.1.3 Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
- 4.1.4 Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
- 4.1.5 Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
- 4.1.6 Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
- 4.1.7 Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo.
- 4.1.8 Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
- 4.1.9 Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
- 4.1.10 Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- 4.1.11 Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
- 4.1.12 Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
- 4.1.13 Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
- 4.1.14 Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
- 4.1.15 Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
- 4.1.16 System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
- 4.1.17 Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
- 4.1.18 Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
- 4.1.19 Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
- 4.1.20 Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
- 4.1.21 Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- 4.1.22 Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
- 4.1.23 Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.

- 4.1.24 Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
- 4.1.25 Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.
- 4.1.26 Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
- 4.1.27 Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
- 4.1.28 Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
- 4.1.29 Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 8 takich procesów przenoszenia jednocześnie.
- 4.1.30 Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
- 4.2 Na potrzeby systemu wirtualizacji Wykonawca dostarczy serwery fizyczne o minimalnych parametrach:
- 4.2.1 minimum 1 serwer fizyczny z 1 procesor minimum 16 rdzeni fizycznych o taktowaniu 2.1Ghz, RAM minimum 128GB 2666MHz, dysk minimum 30 TB pojemności w RAID 5, kontroler RAID minimum 0/1/5/610, karty sieciowe minimum 2 porty RJ45 1Gbps i 2 porty 10Gbps SFP+, zarządzanie zdalne, lub
- 4.2.2 lub równoważne.

5 Parametry techniczne i wymagania minimalne dotyczące dostarczenia i wdrożenia systemu klasy UTM.

5.1 Wymagania ogólne

- 5.1.1 Dostarczony urządzenie musi zapewniać wszystkie wymienione poniżej funkcje.
- 5.1.1.1 Funkcje modułu Firewall:
 - 5.1.1.1.1 musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (zewnętrzna, DMZ1, DMZ2, wewnętrzna1, wewnętrzna2).
 - 5.1.1.1.2 musi umożliwiać pracę jako router lub jako bridge (transparent mode).
 - 5.1.1.1.3 musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP.
 - 5.1.1.1.4 musi obsługiwać Multicast routing.
 - 5.1.1.1.5 musi obsługiwać Policy Based routing.
 - 5.1.1.1.6 musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług
 - 5.1.1.1.7 musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
 - 5.1.1.1.8 musi obsługiwać DHCPv6 na zewnętrznym interfejsie.
 - 5.1.1.1.9 musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
 - 5.1.1.1.10 musi obsługiwać Dynamic DNS.
 - 5.1.1.1.11 musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
 - 5.1.1.1.12 musi obsługiwać IPSec NAT traversal.
 - 5.1.1.1.13 musi obsługiwać mechanizm Policy Based NAT.
 - 5.1.1.1.14 musi obsługiwać VLAN 802.1Q.
 - 5.1.1.1.15 musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
 - 5.1.1.1.16 musi umożliwiać pracę w trybie DHCP Relay.
 - 5.1.1.1.17 musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
 - 5.1.1.1.18 musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
 - 5.1.1.1.19 musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
 - 5.1.1.1.20 musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
 - 5.1.1.1.21 musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
 - 5.1.1.1.22 musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.

- 5.1.1.1.23 musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
- 5.1.1.1.24 musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
- 5.1.1.1.25 musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
- 5.1.1.1.26 musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
- 5.1.1.1.27 musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS, H.323, SIP.
- 5.1.1.1.28 musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
- 5.1.1.1.29 musi zapewniać funkcjonalność TLS/SSL Offloading dla protokołu HTTPS w ramach połączeń do wewnętrznych serwerów.
- 5.1.1.1.30 musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
- 5.1.1.2 Ochrona z wykorzystaniem mechanizmów IPS.
- 5.1.1.3 Ochrona antywirusowa.
- 5.1.1.4 Ochrona przed niechcianą pocztą.
- 5.1.1.5 Kontrola wykorzystywanych aplikacji.
- 5.1.1.6 Możliwość filtrowania URL.

5.2 Wymagane parametry fizyczne:

- 5.2.1 Minimum 4 porty 1Gbps RJ45.
- 5.2.2 Minimum 1 port USB 3.0.

5.3 Wymagane parametry wydajnościowe:

- 5.3.1 Przepustowość Firewall minimum: 1.4 Gbps.
- 5.3.2 Przepustowość IPSec VPN nie mniejsza niż: 400 Mbps.
- 5.3.3 Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 400 Mbps.
- 5.3.4 Obsługa nie mniej niż: 30 tuneli IPSec site-to-site.
- 5.3.5 Obsługa nie mniej niż: 30 tuneli client-to-site.
- 5.3.6 Obsługa nie mniej niż: 3.500.000 jednoczesnych połączeń.
- 5.3.7 Obsługa nie mniej niż: 16.000 nowych połączeń na sekundę.
- 5.3.8 W ramach Firewall system musi obsługiwać minimum: 50 sieci VLAN.

5.4 W ramach ochrony przed atakami system musi zapewniać:

- 5.4.1 Automatyczną aktualizację bazy sygnatur IPS.
- 5.4.2 Automatyczne blokowanie znanych źródeł ataków.
- 5.4.3 Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
- 5.4.4 Mechanizmy ochrony przed atakami typu DoS i DDoS.
- 5.4.5 Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer Overflow, Remote File Inclusions.
- 5.4.6 Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

5.5 W ramach kontroli antywirusowej system musi zapewniać:

- 5.5.1 Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
- 5.5.2 Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
- 5.5.3 Możliwość skanowania plików o rozmiarze co najmniej 20MB.
- 5.5.4 Możliwość zdefiniowania rozmiaru skanowanego pliku.
- 5.5.5 Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
- 5.5.6 Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
- 5.5.7 Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Ransomware, Malware.
- 5.5.8 Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

5.6 W ramach kontroli antyspamowej system musi zapewniać:

- 5.6.1 Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
- 5.6.2 Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
- 5.6.3 Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
- 5.6.4 Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.

5.6.5 Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

5.7 W ramach filtrowania zawartości URL system musi zapewniać:

- 5.7.1 Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
- 5.7.2 Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
- 5.7.3 Odpytywanie bazy on-line w czasie rzeczywistym.
- 5.7.4 Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
- 5.7.5 Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
- 5.7.6 Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
- 5.7.7 Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
- 5.7.8 Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
- 5.7.9 Możliwość filtrowania treści w oparciu o typy MIME.
- 5.7.10 Możliwość blokowania plików cookies dla określonych domen.
- 5.7.11 Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
- 5.7.12 Analizę treści dla protokołu https.
- 5.7.13 Wyłączenie inspekcji https dla wybranych kategorii stron www.

5.8 W ramach kontroli aplikacyjnej system musi zapewniać:

- 5.8.1 Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
- 5.8.2 Ilość rozpoznawanych aplikacji: nie mniej niż 500, podzielonych na kategorie.
- 5.8.3 W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
- 5.8.4 Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
- 5.8.5 Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

5.9 Wymagane funkcje VPN systemu:

- 5.9.1 W zakresie IPsec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
- 5.9.2 Musi wspierać mechanizmy uwierzytelniania: SHA-2, MD5, IKE Pre-Shared Key, certyfikaty.
- 5.9.3 Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
- 5.9.4 Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPsec, SSL, L2TP, IKEv2.
- 5.9.5 Połączenia client-to-site muszą być możliwe z systemów: Windows 7, 8, 10, 11, MacOS, iOS i Android.
- 5.9.6 Dla połączeń IPsec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
- 5.9.7 Dla połączeń Client-to-Site możliwość zastosowania dwuskładnikowego uwierzytelnienia w oparciu o tokeny sprzętowe lub programowe.

5.10 Wymagania dotyczące zarządzania systemem:

- 5.10.1 Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
- 5.10.2 Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
- 5.10.3 Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
- 5.10.4 W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
- 5.10.5 Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
- 5.10.6 Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
- 5.10.7 Komunikacja do systemów logowania i raportowania musi być szyfrowana.
- 5.10.8 W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

5.11 Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

- 5.11.1 Musi zapewniać zarządzanie elementami systemu jednocześnie przez wielu administratorów.
- 5.11.2 Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
- 5.11.3 Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online.

- 5.11.4 Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
- 5.11.5 Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
- 5.11.6 Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
- 5.11.7 System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
- 5.11.8 Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
- 5.11.9 Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
- 5.11.10 Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
- 5.11.11 Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
- 5.11.12 Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
- 5.11.13 Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
- 5.11.14 System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
- 5.11.15 System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
- 5.11.16 Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
- 5.11.17 System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
- 5.11.18 System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
- 5.11.19 Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
- 5.11.20 Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

5.12 Licencje i wsparcie techniczne:

- 5.12.1 W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować: Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów – na minimum 2 lata.
- 5.12.2 System musi być objęty serwisem gwarancyjnym producenta przez minimum 2 lata, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 (świadczone telefonicznie lub poprzez portal).