Załącznik nr 1 rozeznania

1. Szkolenia dla Administratorów – 1 szt.;

Wykonawca musi w terminie do 90 dni od dnia udzielenia zamówienia, dostarczyć Zamawiającemu dokument umożliwiający Zamawiającemu odbycie autorskiego szkolenia:

Urządzenia sieciowe:

- Konfiguracja i zarządzanie
- Zabezpieczenia sieciowe
- Routing i przełączanie
- Zarządzanie jakością usług (QoS)
- Agregacja łączy i redundancja
- Monitoring i zarządzanie
- Aktualizacje i zarządzanie oprogramowaniem
- Zaawansowane techniki diagnostyki i rozwiązywania problemów

Obsługi systemu do backupu danych:

Wykonawca musi w terminie do 90 dni od dnia udzielenia zamówienia, dostarczyć Zamawiającemu dokument umożliwiający Zamawiającemu odbycie autorskiego, jednodniowego szkolenia z obsługi oferowanego oprogramowania do wykonywania kopii zapasowych dla administratora od Zamawiającego. Zakres szkolenia to m.in.:

1. Wstęp do backupu i zarządzania danymi
    - Podstawy backupu i jego znaczenie dla ciągłości działania organizacji.
    - Przegląd dostępnych technologii backupu: backup pełny, przyrostowy, różnicowy.
    - Zasady planowania polityki backupu.
2. Wprowadzenie do systemu do backupu
    - Omówienie architektury systemu do backupu.

- Instalacja i konfiguracja podstawowych komponentów.
- Przegląd interfejsu użytkownika: dashboard, logi, raporty.

3. Tworzenie i zarządzanie zadaniami backupu
   - Definiowanie i tworzenie zadań backupowych.
   - Konfiguracja harmonogramów backupów.
   - Automatyzacja procesów backupu.
   - Testowanie odtwarzania danych (recovery).
4. Zarządzanie przestrzenią dyskową i nośnikami
   - Optymalne wykorzystanie przestrzeni dyskowej.
   - Zarządzanie nośnikami do backupu (taśmy, dyski, chmura).
   - Przechowywanie i rotacja nośników.
   - Polityki retencji danych.
5. Monitorowanie, raportowanie i analiza logów
   - Monitorowanie bieżących zadań backupowych.
   - Przegląd raportów o stanie systemu.
   - Analiza i interpretacja logów systemowych.
   - Sposoby reagowania na błędy i problemy.
6. Odtwarzanie danych (disaster recovery)
   - Proces odtwarzania danych z kopii zapasowych.
   - Testowanie strategii odzyskiwania danych.
   - Najlepsze praktyki w zakresie odtwarzania danych w sytuacjach awaryjnych.
7. Bezpieczeństwo danych w procesie backupu
   - Szyfrowanie danych w backupie.
   - Zarządzanie dostępem do systemu.
   - Audyt i zgodność z politykami bezpieczeństwa.

8. Optymalizacja i automatyzacja procesów backupu
    - Optymalizacja wydajności systemu.
    - Automatyzacja cykli backupu i odzyskiwania.
    - Redukcja kosztów związanych z przechowywaniem danych.

Szkolenia dla 2 osób.

2. Backup - Wdrożenie pełnego systemu kopii zapasowej, modernizacja infrastruktury do backupu, sporządzenie dokumentacji odtworzeniowej – 1 szt.;

W ramach zadania Wykonawca musi zrealizować:

- **uruchomienie specjalistycznego wsparcia IT – 1 szt.**
- **oprogramowanie do wykonywania kopii zapasowych – 1 szt.**

Uruchomienie specjalistycznego wsparcia IT – 1 szt,

Minimalne wymagania:

Zamawiający wymaga wdrożenia strategii tworzenia kopii zapasowych danych, która zapewnia wysoki poziom bezpieczeństwa i odporności na utratę danych.

Pierwszym zadaniem do realizacji jest skonfigurowanie infrastruktury IT Zamawiającego oraz wdrożenie systemu do backupu.

W ramach zadania obowiązkiem Wykonawcy będzie świadczenie specjalistycznego wsparcia IT w zakresie cyberbezpieczeństwa. Wnioskodawca w ramach każdej z zaoferowanych paczek roboczogodzin będzie świadczył specjalistyczne wsparcie IT w min. 30h online w następującym zakresie:

a) Wdrożenie reguł zgodności z przepisami prawnymi oraz standardami bezpieczeństwa.
b) Konfiguracja i zarządzanie firewallami, IDS/IPS i innymi mechanizmami obronnymi.
c) Zarządzanie dostępem i autoryzacją użytkowników.
d) Monitoring sieci i alarmowanie w czasie rzeczywistym.
e) Wdrożenie (na zlecenie) reguł dla Backupu i archiwizacji danych.

f) Szyfrowanie danych wrażliwych.
g) Zabezpieczenie przed oprogramowaniem złośliwym – konfiguracja: antywirus, antimalware.
h) Opracowanie i implementacja planu reagowania na incydenty bezpieczeństwa.
i) Analiza po incydentach i rekomendacje.
j) Stałe monitorowanie logów i zdarzeń związanych z bezpieczeństwem.
k) Zlecone raporty dotyczące stanu bezpieczeństwa.
l) Reagowanie na zgłoszone incydenty związane z bezpieczeństwem
m) Wsparcie w obsłudze wdrożonych systemów

Wszystkie zapisy rozumiane jako doradztwo i konfiguracja urządzeń oraz systemów zakupionych w ramach projektu będą realizowane zgodnie z założonymi incydentami. Incydenty będą mogły być zakładane przez Zamawiającego poprzez udostępnione przez Wykonawcę kanały komunikacji, takie jak co najmniej:

Strona www (24h)
Adres email (24h)
Telefon w dni robocze (7:30 – 15:30) – infolinia w języku polskim.

Dla wsparcia online, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/3) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 3 dni robocze na realizację.

WSPARCIE ONLINE 30h w ramach paczki godzin.
Po zgłoszeniu przez Zamawiającego incydentu - konieczności wsparcia online, Wykonawca ma 3 dni robocze na realizację tego zadania.
Wykonawca musi zaanonsować termin wykonywanych prac w ramach czasu wskazanego na reakcję (1 dzień roboczy).
Wezwanie Wykonawcy do świadczenia usługi wsparcia online odbywać będzie się maksymalnie w ramach 5 zleceń w ramach jednej paczki.
Każda usługa wsparcia online i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego, lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Podpisane protokoły będą podstawą do wystawienia faktur (zgodnie z umową).

Dla zgłoszeń incydentów Zamawiający przekaże wykonawcy imienną listę osób uprawnionych do zgłaszania i raportowania incydentów (maksymalnie 3 osoby).

WYKORZYSTANIE PACZEK GODZIN

W ramach zadania, Wykonawca świadczy na rzecz Zamawiającego usługę specjalistycznego wsparcia IT w 12 paczkach, w wymiarze 30h online (dalej **paczka godzin**), a także pozostaje w trybie gotowości do podjęcia ww. zleceń w okresie o mniejszej intensyfikacji zgłoszeń.

Specjalistyczne wsparcie IT świadczone będzie od dnia podpisania umowy.

Wykonawca przez cały okres świadczenia usługi utrzymuje stan gotowości, do realizacji zleceń – incydentów na rzecz zamawiającego.

Paczka godzin, będzie wykorzystana maksymalnie w ciągu 30 dni.

Okres 30 dni stanowi okres rozliczeniowy dla każdej kolejnej paczki godzin, rozpoczynając od dnia podpisania umowy. Kolejne okresy rozliczeniowe będą liczone od dnia wykorzystania paczki godzin, lub upływie 30 dni.

Zamawiający w okresie 30 dni może wykorzystać maksymalnie 2 paczki godzin. Wykorzystanie większej ilości wsparcia – paczek godzin, może odbyć się tylko za obopólną zgodą Zmawiającego i Wykonawcy.

Wykorzystanie paczki godzin, klasyfikowane będzie zawsze dla okresu, w którym Zamawiający przekazał zgłoszenie incydentu, także w przypadkach, kiedy Wykonawca w jego obsłudze wyszedł poza okres trwania paczki godzin (np. zgłoszenie przekazane w 29 dniu okresu rozliczeniowego pierwszej paczki godzin, obsłużone w 32 dniu będzie zaliczane dla pierwszej paczki godzin).

W przypadku nie wykorzystania wszystkich godzin w ciągu 30 dni, w ramach jednej paczki godzin niewykorzystane godziny nie przechodzą na kolejny okres. Nie zmienia to wynagrodzenia Wykonawcy, pod warunkiem pozostania w gotowości do wykonania zleceń incydentów na rzecz Zamawiającego.

Podmiot realizujący usługę musi posiadać kompetencje z wdrażanego w ramach projektu systemów IT.

<u>Oprogramowanie do wykonywania kopii zapasowych – 1 szt.</u>

Minimalne wymagania:

Rodzaj licencji: wieczysta, ze wsparciem do dnia min. 30-06-2026r.

Oprogramowanie ma zapewnić backup z min. 10 maszyn wirtualnych zaimplementowanych w ramach oferowanych serwerów w niniejszego postępowania.

Wymagania ogólne

Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. 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 i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na

innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)

Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS)

Oprogramowanie musi posiadać integracje z systemami typu SIEM

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

Wymagania RPO

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

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru

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.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu.

Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku.

Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware

Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania

Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Środowiska fizyczne

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego

Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE

Rozwiązanie musi wspierać system operacyjny macOS

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix

Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)

Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów

Rozwiązanie musi wspierać backup podłączonych dysków USB

Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym

Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)

Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone

Rozwiązanie musi wspierać kontrolę pasma sieciowego

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft

Rozwiązanie musi wspierać technologię BitLocker

Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych

Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych

Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform

Rozwiązanie musi wspierać szyfrowanie

Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego

Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej

Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Monitoring

System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn

System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel

System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)

System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna

System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4

Raportowanie

System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF

System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach

System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych

System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury

System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.

System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

3. Modernizacja Data Center serwerowni - Wymiana serwera, dodanie nadmiarowego serwera do infrastruktury,dodanie macierzy dyskowej, uprgrade ram dysków

W ramach zadania wykonawca dostarczy:

- **Serwer –1 szt.,**
- **Macierz dyskowa – 1 szt.**
- **Dodatkowe dyski – 1 kpl.**

Serwer – 1 szt.,

Minimalne wymagania:

Dla serwerów Zamawiający stawia wymagania dot. gwarancji, tj,:

a) Min. 2 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub

autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej

b) Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;

Nazwa elementu, parametru lub cechy	**Opis wymagań Serwerów**
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 16. Minimalna częstotliwość pracy procesora 2.0 GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być nizszy niż 275 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.
Liczba zainstalowanych procesorów	1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum 6 sztuki dysków SSD o pojemności min. 960GB.
Kontroler dyskowy	W momencie dostawy serwer musi posiadać kontroler dyskowy obsługujący dyski zainstalowane dyski. Min poziomy RAID 0, 1, 10, 5, 50, 6, 60. Kontroler musi posiadać wbudowany cache min. 2GB. Kontroler nie może zajmować żadnego ze slotów PCIe wyszczególniuonych w punkcie „Dodatkowe sloty I/O".
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Minimum 2x Port FC (16GB) do połączenia z macierzą

	Minimum 2x port 10GB BaseT do połączenia za switchem
Sloty I/O PCIe	Serwer w momencie dostawy powinien posiadać przynajmniej 2 sloty PCIe x16 generacji 5.
Dodatkowe porty	• z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Wymagana rozszerzona licencja zdalnego kontrolera IPMI (iDrac. iLO itp.) Wymaga się aby serwer posiadał diody sygnalizującę awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu. Wymaga się aby serwer posiadał port diagnostyczny z przodu obudowy umożliwiający podłączenie zewnętrznego panelu diagnostycznego LCD umożlwiającego detekcję usterek. Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Wymagane funkcjonalności kontrolera zdalnego zarządzania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja

	• Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediow z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie

	sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
Funkcje zabezpieczeń	Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0. Zainstalowany przedni panel zabezpieczający, zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.

Dodatkowo do serwera należy dostarczy licencję na system operacyjny o minimalnych parametrach:

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji

wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Dodatkowo system operacyjny musi zawierać 10 licencji dostępowych.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

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

2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18) Mechanizmy logowania w oparciu o:

a) Login i hasło,

b) Karty z certyfikatami (smartcard),

c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.

d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

i. Dystrybucję certyfikatów poprzez http

ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.

g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i) Serwis udostępniania stron WWW.

j) Wsparcie dla protokołu IP w wersji 6 (IPv6),

k) Wsparcie dla algorytmów Suite B (RFC 4869),

l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Macierz dyskowa – 1 szt.

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	Macierz musi mieć możliwość zainstalowania w standardowej szafie rack 19" nie będącej przedmiotem zamówienia. Rozmiar jednostki sterującej macierzą nie może przekraczać 2U . Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo. Całkowity rozmiar dostarczonej macierzy nie może przekraczać 2U.
Kontrolery	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz.

Dostepne porty	Oferowana macierz musi posiadać w chwili dostawy minimum 8 portów 16Gb FC SFP+ powalających na podłączenie serwerów w sposób redundantny (po 4 porty w każdym z kontrolerów)
Cache	Każdy z modułów sterujących musi być wyposażony w min 8 GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania. Rozwiązania wykorzystujące do tego celu tylko i wyłącznie tzw. podtrzymanie cache za pomocą baterii nie są akceptowalne. Bateria może być użyta tylko i wyłącznie na czas zrzutu danych z cache na pamięć nieulotną. Ponadto macierz musi umożliwiać utworzenie dedykowanej przestrzeni SSD stanowiącej pamięć cache pośredniczącą w operacjach odczytów danych z macierzy. Wymaga się możliwości utworzenia takiej przestrzeni o wielkości 4TB.
Dyski	Macierz musi obsługiwać dyski twarde typu SSD oraz dyski obrotowe SAS oraz NL-SAS. Wymaga się możliwości jednoczesnej obsługi przez macierz dysków 3.5 cala oraz dysków 2.5 cala. Macierz musi umożliwiać rozbudowę do minimum 96 sztuk dysków. Macierz wyposażona w min. 12 dysków po 8 TB każdy
Funkcjonalnosc	Macierz musi obsługiwać typy protekcji RAID 0,1,5,6,10 oraz powinna posiadać funkcjonalność zarzadzania informacjami o parzystości oraz dyskami spare w całej puli dysków utworzonej ze wszystkich dysków, które mogą zostać zainstalowane w macierzy. W przypadki awarii dysku, do jego obudowy musi być używany każdy dysk z takiej puli Macierz musi umożliwiać zwiększanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „*thin provisioning*").

	Macierz musi posiadać funkcjonalność sprawdzania integralności zapisywanych danych poprzez odczyt sumy kontrolnej z karty HBA podłączonego serwera. Macierz musi mieć możliwość wykonywania minimum 512 kopii migawkowych typu copy-on-write (jeśli funkcjonalnośc wymaga licencji, nie jest wymagana w momencie dostawy). Macierz musi posiadać funkcjonalność klonowania danych. Wymagana możliwość definiowania maksymalnej ilości kopii migawkowych. W przypadku osiągniecia zdefiniowanej ilości kopii system musi automatycznie kasować kopie najstarsze. Ponadto macierz powinna posiadać funkcjonalność tworzenia konsystentnych kopii migawkowych ze wskazanych przestrzeni dyskowych. Macierz musi mieć możliwość replikacji danych z wykorzystaniem protokołów iSCSI oraz FC w trybie asynchronicznym. Macierz musi pozwalać na wykonanie do 32 jednoczesnych replikacji bez używania systemów zewnętrznych wykonujących replikację. Nie wymaga się funkcjonalności replikacji w momencie dostawy. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji. Wymagana możliwość definiowania globalnych dysków hot-spare. Wymagana możliwość logicznej zamiany dysków z wykorzystaniem dysków nieprzypisanych. Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wysyłane powiadomienia musza zawierać nazwę macierzy, informacje o typie zdarzenia, datę i czas wystąpienia zdarzenia oraz krótki opis zdarzenia. Macierz musi mieć możliwość definowania poziomu zajętości miejsca, po osiągnieciu którego nastąpi wysłanie powiadomienia pod wskazane adresy email.

	System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego automatycznie w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy. Macierz musi mieć funkcjonalność automatycznej detekcji podłączonych hostów (nazwa hosta oraz typ systemu operacyjnego). Musi być możliwość edycji hostów dodanych w sposób automatyczny. Wymagana jest możliwość automatycznego logicznego grupowania dysków macierzy (dodawanie dysków do istniejącej grupy oraz tworzenie nowej grupy z dodanych dysków). Macierz musi mieć możliwość definiowania priorytetu operacji wprowadzanych zmian konfiguracji w odniesieniu do obciążenia generowanego przez podłączone hosty. Wymagana jest możliwość sprawdzenia aktualnych zadań macierzy. Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych. Nie wymaga się tej funkcjonalności w chwili dostawy. Macierz musi posiadać możliwość fizycznej identyfikacji (dioda LED) aktywowanej z interfejsu zarzadzania oraz funkcjonalność fizycznego identyfikowania dysków (dioda LED) należących do jednej przestrzeni logicznej. Macierz musi mieć możliwość przypisania wolumenu danych tylko do wybranego hosta należącego do zdefiniowanego klastra.
Wydajnosc	Wymaga się możliwości rozbudowania macierzy do poziomu wydajności przynajmniej 99 000 operacji wejścia wyjścia dla losowego odczytu oraz przynajmniej 34 000 operacji wejścia wyjścia dla losowego zapisu. Wymagana pojemność dla wolumenów z dynamiczna alokacja przestrzeni to przynajmniej 256 TB

Zarzadzanie macierza	Dostępne dwa porty 1Gbe Base-T w trybie primary/redundant. Zarzadzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh. Interfejs zarzadzania powinien wylogować sesje po maksymalnie 15 minutach bezczynności. Maksymalna ilość prób podania hasła administratora nie może być większa niż 5 do momentu zablokowania dostępu. Wymagana mozliwosc autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: - storage admin – pełen dostęp wyłączeniem ustawień bezpieczeństwa - security admin – dostęp do ustawień bezpieczeństwa - support admin – pełen dostęp serwisowy - monitor – możliwość odczytu konfiguracji Producent powinien udostępniać konsolę umożliwiającą dodawanie do domeny zarzadzania wielu macierzy jednocześnie. Wymaga się możliwości importu konfiguracji z jednej macierzy na inne.
Inne	Wymagana jest bezprzerwowa wymiana następujących elementow macierzy: kontrolery, moduly I/O, dyski, zasilacze oraz moduly SFP+.

	Obsluga systemow operacyjnych hosta: Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES) ; VMware vSphere 7.x, 8.x, Wymaga się dostarczenia wraz z macierzą 4 sztuki kabli Cat6 o długości przynajmniej 3m. Wymaga się możliwości natywnej integracji macierzy z systemem zarządzania infrastrukturą, opisanym w sekcji Serwery bez konieczności jakiegokolwiek skryptowania. Jeśli funkcjonalność wymaga stosownej licencji, jest wymagana w momencie dostawy.
Gwarancja	Co najmniej 3 letnie wsparcie producenta macierzy z czasem reakcji NBD. Serwis w miejscu instalacji sprzętu świadczony przez producenta macierzy lub autoryzowanego partnera serwisowego. W przypadku awarii dyski pozostają własnością Zamawiającego.

Dodatkowe dyski – 1 kpl.

Minimalne wymagania:

Zamawiający wymaga dostarczeni dysków kompatybilnych do już posiadanych urządzeń, wg poniższego zestawienia:

4 sztuki 8TB – QNAP TS-451+ dla CUS

4 sztuki 8TB – TS431U dla UM

4 sztuki 8TB – TS-432PXU dla UM

4. Modernizacja sieci LAN - Modernizacja sieci LAN - wymiana przełączników na zarządzalne switche z NAC oraz wydzielenie VLAN-ów.

W ramach zadania Wykonawca dostarczy:

- **Switch – 4 szt.**
- **UTM – wydłużenie wsparcia – 1 szt.**
- **UTM – dostawa klastra – 1 szt.**

Switch – 4 szt.

Minimalne wymagania:

Przełącznik agregacyjny		
1.	Wymagania ogólne	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
2.	Wymagane parametry fizyczne	Wymagane parametry fizyczne a. możliwość montażu w szafie 19” b. jeden wewnętrzny zasilacze 230V AC c. port USB umożliwiający podłączenie zewnętrznej pamięci flash d. Urządzenie musi cechować się bezwiatrakową obudową (chłodzenie pasywne)
5.	Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: • 48 portów gigabitowych w standardzie 100/1000BaseT

		• Minimum 2 porty typu COMBO 1Gb SFP/RJ45 • Minimum 2 porty typu 10Gb SFP+ Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
6.	Przełącznik	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a. Zarządzanie stosem poprzez jeden adres IP b. Do min. 4 jednostek w stosie c. Magistrala statkująca o wydajności 40 Gb/s d. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie e. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów statkujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą (dwóch dodatkowych niezależnych od portów podstawowych) portów SFP+ w takim wypadku wymagane jest aby z przełącznikiem musi być dostarczony kabel do stackowania 10GE SFP+ od długości minimum 1m. UWAGA: Przełącznik powinien wspierać tzw. in-service software upgrade (ISSU) czyli aktualizację przełączników w stosie bez przerwania pracy całego stosu przełączników
7.	Matryca przełączająca	Matryca przełączająca o wydajności min.

		140 Gbps
8.		Obsługa min 16 000 adresów MAC
9.		Wbudowana pamięć RAM min. 1 GB
10.		Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
11.		Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13.		Obsługa ramek jumbo o wielkości min. 9 216 bajtów
14.		Obsługa protokołu GVRP lub równoważny
15.		Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu.
16.		Obsługa min. 64 tras dla routingu IPv4
17.		Obsługa min. 32 tras dla routingu IPv6
18.		Obsługa protokołów routingu minimum: • IPv4: minimum: statyczny • IPv6: minimum: statyczny
19.		Obsługa protokołów LLDP i LLDP-MED

20.		Przełącznik musi posiadać funkcjonalność DHCP Server
21.		Obsługa ruchu multicast: • IGMP Snooping v1, v2 i v3 • Obsługa 1000 grup multicast
		Obsługa mechanizmu DHCP snooping Obsługa mechanizmu ARP spoof protection
22.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a. min. 4 poziomy dostępu administracyjnego poprzez konsolę b. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www d. zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 e. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP f. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny), g. Możliwość uwierzytelnia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal.

26.	Wymagane opcje zarządzania	a. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, b. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), c. urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, d. dedykowany port konsoli zgodny ze standardem RS-232, e. Obsługa skryptów BASH oraz Python f. Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
27.		Wraz z urządzeniami muszą zostać dostarczone: a. pełna dokumentacja w języku polskim lub angielskim, b. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
28.		Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie

		wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
30.		Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
31.		Przełącznik być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła przełącznik spełniający minimalne parametry techniczne wskazane w niniejszym dokumencie.

UTM – wydłużenie wsparcia – 1 szt.

W ramach zamówienia zamawiający wymaga odnowienia wsparcia na już posiadane urządzenia, tj.:

1. Serial Number : FG100FTK22029548
   Product Model: FortiGate 100F
2. Serial Number : FG80FPTK21001043
   Product Model : FortiGate 80F-PoE

Zamawiający wymaga wydłużenia wsparcia na okres minimum do dnia 30.06.2026r.

Projekt „Poprawa Cyberbezpieczeństwa w Gminie Sępólno Krajeńskie" dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd" z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

UTM – dostawa klastra – 1 szt.

Zamawiający wymaga dostawy nowego urządzania o minimalnych parametrach:

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego

urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.

28. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
29. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
30. Skaner antywirusowy ma pochodzić od europejskiego producenta.
31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
32. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

33. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
34. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
35. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
36. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

37. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
38. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
39. SSL VPN ma działać w trybie tunelu.
40. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
41. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
42. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
43. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.

44. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

45. Urządzenie ma posiadać wbudowany filtr URL.
46. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
47. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
48. Administrator ma mieć możliwość dodawania własnych kategorii URL.
49. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
50. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
51. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
52. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
53. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
54. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
55. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

UWIERZYTELNIANIE

56. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
57. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
58. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.

59. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
60. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
61. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
62. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
63. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
64. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
65. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

66. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
67. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
68. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
69. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
70. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
71. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
72. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

73. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

74. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
75. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
76. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
77. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

ADMINISTRACJA URZĄDZENIEM

78. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
79. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
80. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
81. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
82. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
83. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
84. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
85. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
86. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
88. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
90. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
91. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
92. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
93. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

94. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
95. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
96. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
97. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

98. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
99. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
100. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
101. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
102. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
103. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
104. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
105. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
106. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

107. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
108. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
109. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
110. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

111. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
112. Urządzenie ma posiadać usługę DNS Proxy.
113. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
114. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
115. Urządzenie musi mieć zaimplementowane Open API.
116. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

117. Urządzenie ma być objęte gwarancją producenta min. do dnia 30.06.2026r. na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
118. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

119. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
120. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
121. Liczba portów Ethernet 2,5Gbps – min. 8.
122. Liczba portów światłowodowych 1Gbps – min. 1.
123. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
124. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.
125. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.
126. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.
127. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.
128. Liczba tuneli VPN IPSec – minimum 100.
129. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.
130. Obsługa interfejsów 802.11q (VLAN) – minimum 128
131. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę.
132. Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive.
133. Urządzenie nie ma limitu na liczbę użytkowników.

134. Liczba reguł filtrowania – minimum 8 192.
135. Liczba tras statycznego routingu – minimum 512.
136. Liczba tras dynamicznego routingu – minimum 10 000.
137. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
138. Urządzenie musi być wyposażone w moduł TPM.

5. Bezpieczeństwo na końcówkach - Wdrożenie oprogramowania z modułem XDR, z zewnętrzną usługa Security Office SOCAAS oraz wdrożenie oprogramowania DLP wraz z konfiguracją polityk bezpieczeństwa

W ramach niniejszego zadania Zamawiający wymaga dostarczenie, wdrożenie i konfiguracji wg poniższego zakresu:

- Oprogramowanie klasy SIEM z elementami XDR Extended Detection and Response, EDR Endpoint Detection and Response (jako Centralny System Bezpieczeństwa) – 1 szt.
- Oprogramowanie klasy DLP – 60 szt.

Oprogramowanie klasy SIEM z elementami XDR Extended Detection and Response, EDR Endpoint Detection and Response – 1 szt.

Minimalne wymagania:

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.

Oprogramowanie musi posiadać wsparcie min. do dnia 30-06-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.

Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.

Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.

Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kątem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).

Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.

Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.

Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.

Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.

Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.

Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).

Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.

Odkrywanie i Analiza Danych: System musi umożliwiać użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.

Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.

Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.

Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie.

Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.

Zgodność ze standardami HTML i CSS całego serwisu www.

Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA.

System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

1. **MODUŁ ANALIZY PODATNOŚCI**

1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.
Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności "nowe", których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

1.2. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

1.3. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na

nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

2. MODUŁ MONITORINGU ZASOBÓW

2.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami

System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

2.3. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach

System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w

przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów

Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko "nowe" problemy i zdarzenia oraz te, których status nie został zmieniony na "rozwiązany" bądź "anulowany". Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, system przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: "help-desk", przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej

Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT

System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np.

brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT

System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.8 Zdalny dostęp do urządzeń końcowych

System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.

2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych

System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i

wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.

2.10 Analiza ruchu sieciowego

System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.

2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach

System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

3. MODUŁ ANALIZY LOGÓW

3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

3.2. Możliwość analizy tzw. „customowych" logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.

System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. "customowych" logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany

z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.

3.3. Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzinowego - "customlogów"), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

3.4. Przegląd i analiza logów dotyczących działań użytkowników.

W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

3.6. Dostęp do logów historycznych.

System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

3.7. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu

w lagach oraz wyboru typu logu (m.in. log systemowy, log "customowy"). Ponadto CSB musi informować użytkownika/administratora o "nowych" zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a "nowe" logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

3.8. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).

System musi być wyposażony w mechanizmy kategoryzujące logi pod kątem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

4. **MODUŁ EDR/XDR**

4.1 System musi posiadać własny moduł EDR/XDR, czyli zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.

4.2 Moduł musi posiadać podgląd informacji, alertów i zdarzeń występujących w środowisku IT. W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

4.3 Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender, Arcabit). System musi umożliwiać bezpośrednie przekierowanie do

zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.

5. MODUŁ INWENTARYZACJI

5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez "ręczne" wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.

5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja)

Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu "ręcznym" system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

5.3. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać

m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

6. MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)

6.1. Integracja z systemem tiketowym.

System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

6.2. Zgłaszanie incydentu/problemu, który został namierzony przez system.

Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku "Zgłoś Problem". Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

6.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

7. MODUŁ WYKRYWANIA ZAGROŻEŃ

7.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.

System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

7.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń

System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.

7.3. Historia wykrytych zagrożeń

System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).

7.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia

System musi posiadać możliwość włączenia "automatycznej ochrony" w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykonana w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta na którym występuje zagrożenie.

8. MODUŁ RAPORTÓW

8.1. Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów

System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik (z odpowiednimi uprawnieniami) musi mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

9. PANEL UŻYTKOWNIKA

9.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

9.2. Wizualizacja statystyk zdarzeń i logów

Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości "nowych" zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

9.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo".

Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na "żywo", a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

9.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

9.5. Intuicyjny panel zarządzania regułami i definiowania "customowych" logów.

Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania "customowymi" logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych "customlogów" wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu "customlogów" musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.

Dodatkowo w ramach wdrożenie niniejszego oprogramowania Zamawiający wymaga dostosowanie usług katalogowych dla użytkowników, wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa.

Obowiązkiem Wykonawcy jest omówienie harmonogramu wykonania usługi z Zamawiającym.

W harmonogramie powinna znaleźć się informacja o anonsowaniu planowanych prac przez Wykonawcę i forma jej potwierdzenia przez Zamawiającego. Harmonogram musi być zaakceptowany przez strony.

1.1 Wdrożenie i skonfigurowanie usług katalogowych musi zapewniać efektywne zarządzania dostępem do zasobów informatycznych u Zamawiającego. Obowiązkiem Wykonawcy będzie utworzenie struktury organizacyjnej, grup, kont użytkowników oraz polityk bezpieczeństwa. Szczegółowy zakres prac zawiera:

a. Analiza i Projektowanie:
- Ocena infrastruktury istniejącej w celu dostosowania projektu do istniejących zasobów.
- Zaprojektowanie struktury organizacyjnej usług katalogowych z uwzględnieniem potrzeb Zamawiającego.

Efektem działań będzie utworzenie dokumentu zawierającego ustalaną strukturę usług katalogowych. Dokument ten zostanie zatwierdzony przez zamawiającego w celu kontynuowania prac.

b. Wdrożenie:
- Instalacja na infrastrukturze Zamawiającego (serwerach z oprogramowaniem).
- Konfiguracja globalnych i lokalnych polityk bezpieczeństwa.
- Utworzenie grup użytkowników i przydzielanie odpowiednich uprawnień.
- Integracja usługi z istniejącymi systemami.
- Wpięcie urządzeń klienckich wytypowanych przez Zamawiającego, wraz z przeniesieniem profili użytkownika.
- Wsparcie w rozwiązaniu problemów związanych z wdrażaniem urządzeń klienckich.

Efektem działań będzie przekazanie maszyny z zainstalowaną i skonfigurowaną usługą katalogową.

c. Testowanie i akceptacja:
- Przeprowadzenie testów funkcjonalnych w celu potwierdzenia poprawności działania usługi katalogowej.
- Protokolarne przekazanie dokumentacji dotyczącej konfiguracji, w tym haseł dostępowych instrukcji i postępowania w razie problemów.

1.2 Wdrożenie oferowanego Centralnego Systemu Bezpieczeństwa (dalej CSB), polegające w szczególności na instalacji oraz uruchomieniu rozwiązania. Do obowiązków Wykonawcy należeć będą:

a) Instalacja fizyczna i konfiguracja funkcjonalna komponentów systemu CSB.

b) Konfiguracja systemu CSB w środowisku Zamawiającego. Zdefiniowanie niezbędnych do poprawnego działania systemu parametrów konfiguracyjnych.
c) Integracja z usługą katalogową w zakresie autentykacji użytkowników. Konfiguracja ról Użytkowników.
d) Podłączenie do 3 rodzajów źródeł zdarzeń (np. UTM, switch, serwer) rozpoznawanych przez system CSB. Wykonawca przekaże wytyczne dla Zamawiającego dotyczące koniecznej konfiguracji źródeł zdarzeń Zamawiającego.
e) Budowa minimum 1 parser dla źródeł zdarzeń nieobsługiwanych automatycznie przez system CSB.
f) Możliwość tworzenia niestandardowych reguł korelacyjnych/scenariuszy oraz aktywacja/konfiguracja wbudowanych reguł korelacyjnych
g) Konfiguracja polityk retencji danych
h) Przygotowanie dokumentacji powykonawczej, zawierającej co najmniej zbiór haseł dostępowych, instrukcji i postępowania w razie problemów
i) Przygotowanie i przetestowanie procedur kopii bezpieczeństwa i odtwarzania systemu po awarii
j) Instalacja najnowszej wersji składników systemu

Efektem wdrożenia musi być działanie CSB (systemu klasy SIEM) w środowisku IT Zamawiającego. Dodatkowe konfiguracje (aktualizacje) będą wykonywane w ramach Specjalistycznego wsparcia IT opisanego w dalszej części dokumentu.

Oprogramowanie klasy DLP – 60 szt.

Minimalne wymagania:

Licencja na okres min. do 30.06.2026r.

Minimalne wymagania dla systemu:

- Monitorowanie i kontrola danych: Śledzenie przepływu danych w organizacji, zarówno wewnątrz sieci, jak i podczas ich przesyłania na zewnątrz (np. przez e-maile, urządzenia zewnętrzne, chmurę).
- Ochrona danych wrażliwych: Identyfikacja i klasyfikacja danych poufnych, takich jak dane osobowe, finansowe czy intelektualna własność, oraz blokowanie ich nieautoryzowanego przesyłu.

- Regulowanie dostępu: Ustalanie polityk bezpieczeństwa, które definiują, kto ma dostęp do danych oraz jakie działania mogą być wykonywane (np. kopiowanie, drukowanie).
- Blokowanie i ostrzeganie: Automatyczne blokowanie prób nieautoryzowanego transferu danych lub wysyłanie ostrzeżeń administratorom systemu.
- Raportowanie i audyt: Tworzenie szczegółowych raportów o naruszeniach i potencjalnych zagrożeniach, co ułatwia analizę i zgodność z przepisami prawnymi.

6. Backup - Jeden dodatkowy serwer, szafa rack, 2 NASy , 2 dyski ok 8-10 TB z przeznaczeniem do CMDiR, CSiR

W ramach zadania Zamawiajacy wymaga dostarczenia:

- **Serwer – 1 sz.**
- **Szafa rack – 1 szt.**
- **NAS – 2 szt.**
- **UPS serwerowy – 2 szt.**
- **NAS Tower – 2 szt.**
- **UPS Stanowiskowy – 15 szt.:**

Serwer – 1 sz.

Minimalne wymagania:

Dla serwerów Zamawiający stawia wymagania dot. gwarancji, tj,:

c) Min. 2 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej
d) Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;

Nazwa elementu, parametru lub cechy	**Opis wymagań Serwerów**
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 16. Minimalna częstotliwość pracy procesora 2.0 GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być nizszy niż 275 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.
Liczba zainstalowanych procesorów	1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum 6 sztuki dysków SSD o pojemności min. 960GB.
Kontroler dyskowy	W momencie dostawy serwer musi posiadać kontroler dyskowy obsługujący dyski zainstalowane dyski. Min poziomy RAID 0, 1, 10, 5, 50, 6, 60. Kontroler musi posiadać wbudowany cache min. 2GB. Kontroler nie może zajmować żadnego ze slotów PCIe wyszczególniuonych w punkcie „Dodatkowe sloty I/O".

Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Minimum 2x Port FC (16GB) do połączenia z macierzą Minimum 2x port 10GB BaseT do połączenia za switchem
Sloty I/O PCIe	Serwer w momencie dostawy powinien posiadać przynajmniej 2 sloty PCIe x16 generacji 5.
Dodatkowe porty	• z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Wymagana rozszerzona licencja zdalnego kontrolera IPMI (iDrac. iLO itp.) Wymaga się aby serwer posiadał diody sygnalizującę awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu. Wymaga się aby serwer posiadał port diagnostyczny z przodu obudowy umożliwiający podłączenie zewnętrznego panelu diagnostycznego LCD umożlwiającego detekcję usterek. Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Wymagane funkcjonalności kontrolera zdalnego zarządzania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu,

	wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediow z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą)

	bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
Funkcje zabezpieczeń	Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0. Zainstalowany przedni panel zabezpieczający, zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.

Dodatkowo do serwera należy dostarczy licencję na system operacyjny o minimalnych parametrach:

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Dodatkowo zamawiający wymaga 30 licencji dostępowych.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

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

2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18) Mechanizmy logowania w oparciu o:

a) Login i hasło,

b) Karty z certyfikatami (smartcard),

c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.

d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

i. Dystrybucję certyfikatów poprzez http

ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.

g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i) Serwis udostępniania stron WWW.

j) Wsparcie dla protokołu IP w wersji 6 (IPv6),

k) Wsparcie dla algorytmów Suite B (RFC 4869),

l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Szafa rack – 1 szt.

Minimalne wymagania:

Szafa RACK 19" 42U stojąca 600x1000 kompatybilna z zaoferowanym sprzętem.

Wymiary montażowe: 19" x 42U x 760mm

Zamykanie:

- drzwi frontowe – zamek z kompatybilnym kluczykiem

- drzwi tylne – zamek z kompatybilnym kluczykiem

- drzwi boczne – Click (możliwość montażu zamka)

Wykonanie – Stal walcowana na zimno SPCC w kolorze czarnym

W zestawie 4 kółka bez blokady i nogi poziomujące

Możliwość przełożenia drzwiczek lewa / prawa

Gwarancja producenta na co najmniej 12 miesięcy, gwarancja Wykonawcy na co najmniej 24 miesiące.

NAS – 2 szt.

Minimalne wymagania:

Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu min 2,0 GHz
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA
HDD	NAS wyposażony w min. 5 szt. HDD 16TB każdy
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8

Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 4-liniowe gniazdo x8
Wentylator obudowy	Min. 2 wentylatory 80 mm x 80 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2 048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)

Wirtualizacja	Obsługa m.in.: VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń.
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach

	publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.
Konserwacja	• Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Gwarancja producenta	• Min. 2 lata

UPS serwerowy – 2 szt.

1) Moc pozorna - 3000 VA
2) Moc rzeczywista - 3000 W
3) Topologia (klasyfikacja IEC 62040-3) - Line-interactive z AVR
4) Współczynnik mocy – 1
5) Czas przełączenia na baterię - <4 ms
6) Liczba, typ gniazd wyjściowych - 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
7) Typ gniazda wejściowego - IEC C20 16A
8) Czas podtrzymania dla 2500W obciążenia - 3 min
9) Czas podtrzymania przy 1200W obciążenia -9 min
10) Napięcie znamionowe - 200/208/220/230/240/250 V
11) Tolerancja napięci prostownika - 160 V – 294 V (regulacja programowa 150-294 V)
12) Częstotliwość znamionowa - 50/60 Hz autodetekcja

13) Tolerancja częstotliwości - 47– 70 Hz
14) Kształt napięcia – Sinusoidalny
15) Napięcie znamionowe wyjściowe - 200/208/220/230/240 V do wyboru przez użytkownika
16) Zakres zmian napięcia - +6/-10% napięcia nominalnego
17) Częstotliwość wyjściowa - 50/60 Hz
18) Współczynnik szczytu - 3:1
19) Baterie wymieniane przez użytkownika "na gorąco" – Tak
20) Ochrona przed przeładowaniem - Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
21) Ochrona przed głębokim rozładowaniem - Tak
22) Okresowy automatyczny test baterii – Tak
23) System zarządzania pracą baterii
24) Możliwość uruchomienia bez napięcia w sieci "zimny start" – Tak
25) Baterie wewnętrzne o pojemności nie mniejszej niż - 9Ah 12V, minimum 6 szt.
26) Czas ładowania baterii do poziomu 90% - < 3 godz. do 90% pojemności użytkowej
27) Interfejs komunikacyjny:

a) USB
b) RS232 DB-9 żeński (HID)
c) styki przekaźnikowe
d) miniport wyłącznik ON/OFF
e) SNMP/Ethernet

28) Panel sterowania z wyświetlaczem LCD:

a) Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
b) Poziomy rząd przycisków sterowania
c) Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
d) Sygnalizator akustyczny

29) Sygnały akustyczne, co najmniej na awarię, niski stan naładowania baterii, przeciążenie, oraz konieczność serwisu.
30) Przyciski sterujące i wskaźniki diodowe LED, co najmniej Przycisk Escape (anulowanie), Przyciski funkcyjne (przewijanie w górę i w dół), Przycisk Enter (potwierdzający), Przycisk ON/OFF załączenia i wyłączenia, LED trybu zasilania z siec i(kolor zielony), LED trybu baterii (kolor żółty), LED usterki (kolor czerwony).
31) Typ obudowy uniwersalna Tower/Rack 2U
32) Dane techniczne karty SNMP:

a) Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
b) Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
c) Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
d) Kamptybilność: SNMP v1/v3 i IP v4/v6
e) Interfejs: HTML5
f) Adresowanie IP: DHCP/BootP/Manualne
g) Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
h) Dostępny port USB (microUSB - port serwisowy)
i) Certyfikaty: UL 2900-1, 2900-2-2

33) Dołączone oprogramowanie - Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów operacyjnych.
34) Poziom hałasu w odl. 1m - do 40 dBA dla pracy normalnej
35) Znaki bezpieczeństwa - CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
36) Możliwość montażu ręcznego bypassu serwisowego
37) Gwarancja producenta - 36 miesięcy dla elektroniki, 24 miesiące dla baterii

NAS Tower – 2 szt.

Specyfikacja sprzętowa	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 4 zatoki 3,5" Wymagana dostawa min 3 szt. dysków każdy po 6 TB
Obsługiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD

Wbudowane w urządzenie interfejsy na dyski M2	Wymagane min. 2 x M2 PCIe Gen3x1
Możliwość stosowania dysków twardych o pojemności	do 18TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 3
Port PCiE	Tak, minimum 2 Gen3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek

Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN

Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS

Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

UPS Stanowiskowy – 15 szt.:

Moc pozorna 900 VA

Moc rzeczywista 480 W

Technologia Line-Interactive

Gniazda wyjściowe z podtrzymaniem bateryjnym typu E (2P+Z), minimum 2szt

Przewód zasilający Przymocowany na stałe do zasilacza UPS

Port komunikacyjny USB umieszczony na przednim panelu zasilacza UPS

Wskaźnik stanu UPS Dioda LED

Parametry wejściowe

Napięcie znamionowe 220-240 V; 50/60 Hz

Zakres napięcia wejściowego 140-300 V; 45-65 Hz

Parametry wyjściowe

Znamionowe napięcie wyjściowe 220/230/240 V

Regulacja napięcia w trybie bateryjnym +/-20%

Sprawność w trybie normalnym>95%

Sprawność w trybie bateryjnym>60%

Regulacja częstotliwości w trybie normalnym zgodnie z siecią zasilającą

Regulacja częstotliwości w trybie bateryjnym +/-1 Hz

Częstotliwość w trybie normalnym zgodnie z siecią zasilającą

Częstotliwość w trybie bateryjnym 50/60 Hz

Przeciążalność [110%,120%] 5 min; >120% 1 s

Zdolność zwarciowa w trybie bateryjnym 5A

Wytrzymywany czas przepływu prądu zwarciowego 50 ms

Czas przełączania 10 ms dla przejścia z trybu normalnego do trybu bateryjnego

Bateria

Specyfikacja 12 V DC – 1 x 12 V, 7 Ah

Typ Valve Regulated Lead-Acid (VRLA) szczelne, bezobsługowe, z minimalną żywotnością 3 lat w temperaturze 25°C

Monitoring Zaawansowany monitoring z wczesnym wykrywaniem awarii oraz powiadamianiem.

Zimny start Tak

Stopień ochrony IP20

Gwarancja 24 miesiące