

## Opis przedmiotu zamówienia

### Uwaga wstępna:

Wszędzie tam, gdzie w opisie przedmiotu zamówienia, w tym załącznikach do SWZ znajdują się określenia wskazujące znaki towarowe, patenty lub pochodzenie, źródła lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę zamawiający dopuszcza możliwość zaoferowania przez Wykonawców produktów, materiałów lub urządzeń równoważnych. Użyte nazwy, typy, należy traktować jako rozwiązania przykładowe określające kryteria stosowane w celu oceny równoważności tj. standardy jakościowe, wygląd i parametry techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakie muszą spełniać rozwiązania równoważne, aby spełnić wymagania stawiane przez Zamawiającego. Jako równoważne dopuszcza się inne rozwiązania, niż podane w dokumentach zamówienia, pod warunkiem spełnienia kryteriów stosowanych w celu oceny równoważności tj. zagwarantowania równorzędnych parametrów technicznych i technologicznych nie gorszych niż określone w dokumentach zamówienia oraz zgodności z obowiązującymi wymaganiami prawnymi. Podane typy i właściwe im cechy mogą jedynie służyć dla lepszego doboru zamienników.

W przypadku, gdy w opisie przedmiotu zamówienia zostały zastosowane odniesienia do norm, ocen technicznych, specyfikacji technicznych i systemów referencyjnych, o których mowa w art. 101 ust. 1-3 Ustawy, zamawiający zgodnie z art. 101 ust. 4 Ustawy dopuszcza zastosowanie rozwiązań równoważnych. Każdorazowo, gdy wskazana jest w niniejszej SWZ norma, ocena techniczna, specyfikacja techniczna lub system referencji technicznych należy przyjąć, że w odniesieniu do nich użyto sformułowania „lub równoważne”.

Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie tj. materiały, urządzenia, dostawy, usługi spełniają wymagania, określone w opisie przedmiotu zamówienia przez Zamawiającego (tj. normy, oceny techniczne, specyfikacje techniczne i systemy referencji technicznych), a ciężar udowodnienia równoważności w stosunku do wymogu określonego przez Zamawiającego, spoczywa na Wykonawcy, w szczególności przy pomocy przedmiotowych środków dowodowych, o których mowa w art. 104-107 ustawy Pzp.

W ramach realizacji zamówienia Wykonawca zobowiązany jest dostarczyć rozwiązania (sprzęt, oprogramowanie, usługi), które nie są wytworzone ani dostarczane przez podmioty znajdujące się w wykazie dostawców wysokiego ryzyka publikowanym w Dzienniku Urzędowym Rzeczypospolitej Polskiej "Monitor Polski", na podstawie decyzji, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r., poz. 20 ze zm., dalej „KSC”). Wykonawca na wezwanie Zamawiającego przedstawi wykaz producentów oraz kraj pochodzenia oferowanych kluczowych komponentów ICT.

Wykonawca ma obowiązek zweryfikować w zakresie dostarczanego przedmiotu zamówienia, że kody źródłowe i/lub infrastruktura chmurowa (jeśli dotyczy) nie są kontrolowane przez dostawcę wysokiego ryzyka, w rozumieniu KSC.

**Przedmiot obejmuje kompleksowe rozwiązanie, składające się z:**

1. NGFW (Next Gen FireWall) – 2 szt. NGFW typ I oraz 2 szt. NGFW typ II;
2. Serwera fizycznego niezbędnego do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA – 2 szt. serwer fizyczny;
3. Zarządzalnego urządzenia sieciowego z obsługą VLAN, MACsec, standardu 802.1x (switch) – 5 szt. switch typ I, 2 szt. switch typ II;
4. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise – 6 szt.;
5. Oprogramowania / licencji NAC ( Network Access Control) – licencja obejmująca 150 urządzeń końcowych;
6. Systemu operacyjnego, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 2 szt. system operacyjny;
7. Licencje dostępowe do systemu, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – licencje dla 60 użytkowników;
8. Oprogramowania / licencji IDS (Intrusion Detection System) dedykowanego sieciom OT – 1 szt. licencji;
9. Oprogramowania SIEM (Security Information and Event Management) – 1 szt. licencji;
10. Network Attached Storage (NAS) – 2 szt. NAS;
11. Systemu wirtualizacyjnego dedykowanego do systemów, na których zostanie zainstalowany produkt z zakresu cyberbezpieczeństwa – 1 szt. licencji;
12. Serwera do wykonywania kopii zapasowych – 1 szt. serwera do backupu;
13. Usługi kopii zapasowych w chmurze obliczeniowej IT/OT/ICS – licencja na usługę kopii zapasowych w chmurze obliczeniowej min. 4TB;
14. Oprogramowania do monitorowania infrastruktury informatycznej – 1 szt. licencji;
15. Wdrożenia oprogramowania z zakresu bezpieczeństwa – wdrożenia systemu typu opensource do analizy powłamaniowej;
16. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa – 2 szt. UPS;
17. Szafy RACK do produktów i rozwiązań z zakresu bezpieczeństwa – 1 szt.;
18. Wdrożenia urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa;
19. Usługi konfiguracji i hardeningu systemów/urządzeń;

**I. NGFW (Next Gen FireWall) – 2 szt. NGFW typ I oraz 2 szt. NGFW typ II;**

**NGFW typ I – 2 szt.**

1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach

Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat.

3. Urządzenie musi umożliwiać działanie w następujących trybach pracy:
  - a. rutera (tzn. w warstwie 3 modelu OSI),
  - b. mostu (tzn. w warstwie 2 modelu OSI),
  - c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych i musi pracować w trybie przezroczystego łączenia interfejsów w pary),
  - d. w trybie pasywnego nasłuchu (sniffer/tap).
4. System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. Urządzenie musi być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 Mbps.
6. Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
7. Urządzenie firewall musi posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
8. Urządzenie firewall musi posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
9. Urządzenie firewall musi wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
10. Urządzenie firewall musi wspierać protokół LACP.
11. Urządzenie firewall musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
12. Urządzenie firewall musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
13. Polityka zabezpieczeń firewall musi uwzględniać
  - a. adresy IP źródłowe i docelowe,
  - b. protokoły i usługi sieciowe,
  - c. aplikacje,
  - d. kategorie URL,
  - e. użytkowników aplikacji i grupy,
  - f. reakcje zabezpieczeń,

- g. logowanie zdarzeń (początek i koniec sesji),
  - h. strefa wejściowa i wyjściowa.
14. Urządzenie firewall musi automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
  15. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
  16. Urządzenie firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
  17. Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.
  18. Urządzenie firewall musi być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
  19. Urządzenie firewall musi być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów.
  20. Dostęp do urządzenia i zarządzania z sieci musi być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
  21. Urządzenie firewall musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
  22. Urządzenie firewall musi zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
    - a. Active Directory,
    - b. Terminal Services.
  23. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.

24. Urządzenie firewall musi pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
25. Urządzenie firewall musi umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
26. Urządzenie firewall musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
  - a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia),
  - b. API.
27. Urządzenie firewall musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
28. Urządzenie firewall musi obsługiwać protokoły routingu dynamicznego, minimum: BGP, RIP, OSPF dla IPv4 i IPv6.
29. Urządzenie firewall musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
30. Urządzenie firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
31. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
32. Urządzenie firewall musi pozwalać na selektywne wysyłanie logów do zewnętrznych systemów (np. Syslog) w zależności od ich rodzaju.
33. Urządzenie firewall musi obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
34. Urządzenie firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
35. Wykonywanie operacji deszyfrowania ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.



36. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
37. Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
38. Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
39. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS\_AES\_128\_GCM\_SHA256, TLS\_AES\_256\_GCM\_SHA384 oraz TLS\_CHACHA20\_POLY1305\_SHA256.
40. Urządzenie firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
41. Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
42. Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
43. Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
44. Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesję w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
45. Urządzenie firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPsec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
46. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
47. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
48. Urządzenie firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
49. Urządzenie firewall musi obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPsec.
50. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
51. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS

52. Jeżeli oprogramowanie klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.
53. Urządzenia firewall muszą posiadać funkcję filtrowania URL.
54. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
55. Urządzenie firewall musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
56. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
57. Urządzenie firewall musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
58. Urządzenie firewall musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co firewall.
59. Urządzenie firewall musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
60. Urządzenie firewall musi posiadać funkcję ochrony DNS. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
61. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.
62. Rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznannej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w chmurze producenta, przy czym:
  - a. wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
  - b. analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 muszą być możliwe minimum dla ruchu typu: http, http2, ssl oraz niezidentyfikowanych przez firewall aplikacji w oparciu o TCP i UDP.
63. Kategoryzacja URL musi być realizowana w oparciu o:
  - a. Bazę kategorii utrzymywaną i aktualizowaną przez producenta składającą się z co najmniej 70 kategorii)
  - b. Lokalny mechanizm kategoryzacji stron działający na bazie nauczania maszynowego (Machine Learning - ML)

- c. Zdalny mechanizm kategoryzacji stron działający na bazie nauczania maszynowego (Machine Learning - ML)
- 64. Wyżej wymienione opcje kategoryzacyjne oparte o nauczanie maszynowe (Machine Learning -ML) powinny wykrywać i zapewniać ochronę przed złośliwymi stronami / atakami Phishing, złośliwymi skryptami JavaScript.
- 65. System musi posiadać co najmniej 500 predefiniowanych wzorców danych umożliwiających identyfikację różnorodnych typów informacji
- 66. System powinien wykorzystywać klasyfikatory ML (Machine Learning) do analizy i klasyfikacji danych w celu zwiększenia skuteczności wykrywania.
- 67. System musi umożliwiać stosowanie wbudowanych profili filtrowania danych zgodnych z wymaganiami prawnymi, takimi jak RODO (GDPR), CCPA, PII
- 68. System powinien umożliwiać definiowanie i stosowanie poziomów pewności dopasowania
- 69. System musi umożliwiać podejmowanie działań w czasie rzeczywistym, takich jak blokowanie lub generowanie alertów dla ruchu sieciowego (inline traffic)
- 70. W przypadku gdy jakkolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres do 31.12.2026r.

#### Parametry sprzętowe

1. Urządzenie musi być wyposażone w minimum:
  - a. 1G (8),
2. Urządzenie musi być wyposażone w zasób dyskowy, inny niż obrotowy HDD, o pojemności minimum 128 GB eMMC na potrzeby systemu operacyjnego i logów.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
  - a. Minimum 4.6 Gbps dla rozpoznawania i kontroli aplikacji,
  - b. Minimum 3.0 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,
  - c. Minimum 67.000 nowych sesji na sekundę,
  - d. Minimum 400.000 równoległych sesji.
4. Urządzenie musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tablice routingu.

#### Warunki serwisu technicznego i procedura zgłoszeń

1. Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.
2. Wsparcie techniczne musi być świadczone przez okres do 31.12.2026r.
3. W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej



producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.

### NGFW typ II – 2 szt.

1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat.
3. Urządzenie musi umożliwiać działanie w następujących trybach pracy:
  - a. rutera (tzn. w warstwie 3 modelu OSI),
  - b. mostu (tzn. w warstwie 2 modelu OSI),
  - c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych i musi pracować w trybie przezroczystego łączenia interfejsów w pary),
  - d. w trybie pasywnego nasłuchu (sniffer/tap).
4. System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. Urządzenie musi być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 Mbps.
6. Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
7. Urządzenie firewall musi posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
8. Urządzenie firewall musi posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
9. Urządzenie firewall musi wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
10. Urządzenie firewall musi wspierać protokół LACP.
11. Urządzenie firewall musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
12. Urządzenie firewall musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w

regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.

13. Polityka zabezpieczeń firewall musi uwzględniać

- a. adresy IP źródłowe i docelowe,
- b. protokoły i usługi sieciowe,
- c. aplikacje,
- d. kategorie URL,
- e. użytkowników aplikacji i grupy,
- f. reakcje zabezpieczeń,
- g. logowanie zdarzeń (początek i koniec sesji),
- h. strefa wejściowa i wyjściowa.

14. Urządzenie firewall musi automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).

15. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.

16. Urządzenie firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.

17. Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.

18. Urządzenie firewall musi być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.

19. Urządzenie firewall musi być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów.

20. Dostęp do urządzenia i zarządzania z sieci musi być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

21. Urządzenie firewall musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu

- administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
22. Urządzenie firewall musi zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
- Active Directory,
  - Terminal Services.
23. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
24. Urządzenie firewall musi pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
25. Urządzenie firewall musi umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
26. Urządzenie firewall musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
- reakcji na zdarzenie/log (np. wystąpienie zagrożenia),
  - API.
27. Urządzenie firewall musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMware ESX i VMware vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
28. Urządzenie firewall musi obsługiwać protokoły routingu dynamicznego, minimum: BGP, RIP, OSPF dla IPv4 i IPv6.
29. Urządzenie firewall musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
30. Urządzenie firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
31. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.

32. Urządzenie firewall musi pozwalać na selektywne wysyłanie logów do zewnętrznych systemów (np. Syslog) w zależności od ich rodzaju.
33. Urządzenie firewall musi obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
34. Urządzenie firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielną od polityk bezpieczeństwa.
35. Wykonywanie operacji deszyfrowania ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
36. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
37. Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
38. Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
39. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS\_AES\_128\_GCM\_SHA256, TLS\_AES\_256\_GCM\_SHA384 oraz TLS\_CHACHA20\_POLY1305\_SHA256.
40. Urządzenie firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
41. Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
42. Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
43. Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
44. Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesję w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
45. Urządzenie firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPsec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
46. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

47. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
48. Urządzenie firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
49. Urządzenie firewall musi obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec.
50. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
51. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS
52. Jeżeli oprogramowanie klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.
53. Urządzenia firewall muszą posiadać funkcję filtrowania URL.
54. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
55. Urządzenie firewall musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
56. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
57. Urządzenie firewall musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
58. Urządzenie firewall musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co firewall.
59. Urządzenie firewall musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
60. Urządzenie firewall musi posiadać funkcję ochrony DNS. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
61. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.
62. Rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznannej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w chmurze producenta, przy czym:



- c. wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
  - d. analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 muszą być możliwe minimum dla ruchu typu: http, http2, ssl oraz niezidentyfikowanych przez firewall aplikacji w oparciu o TCP i UDP.
63. Kategoryzacja URL musi być realizowana w oparciu o:
- a. Bazę kategorii utrzymywaną i aktualizowaną przez producenta składającą się z co najmniej 70 kategorii)
  - b. Lokalny mechanizm kategoryzacji stron działający na bazie nauczania maszynowego (Machine Learning - ML)
  - c. Zdalny mechanizm kategoryzacji stron działający na bazie nauczania maszynowego (Machine Learning - ML)
64. Wyżej wymienione opcje kategoryzacyjne oparte o nauczanie maszynowe (Machine Learning -ML) powinny wykrywać i zapewniać ochronę przed złośliwymi stronami / atakami Phishing, złośliwymi skryptami JavaScript.
65. System musi posiadać co najmniej 500 predefiniowanych wzorców danych umożliwiających identyfikację różnorodnych typów informacji
66. System powinien wykorzystywać klasyfikatory ML (Machine Learning) do analizy i klasyfikacji danych w celu zwiększenia skuteczności wykrywania.
67. System musi umożliwiać stosowanie wbudowanych profili filtrowania danych zgodnych z wymaganiami prawnymi, takimi jak RODO (GDPR), CCPA, PII
68. System powinien umożliwiać definiowanie i stosowanie poziomów pewności dopasowania
69. System musi umożliwiać podejmowanie działań w czasie rzeczywistym, takich jak blokowanie lub generowanie alertów dla ruchu sieciowego (inline traffic)
70. W przypadku gdy jakkolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres do 31.12.2026r.

#### Parametry sprzętowe

- 5. Urządzenie musi być wyposażone w minimum:
  - a. 1G (8),
- 6. Urządzenie musi być wyposażone w zasób dyskowy, inny niż obrotowy HDD, o pojemności minimum 128 GB eMMC na potrzeby systemu operacyjnego i logów.
- 7. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
  - a. Minimum 1.5 Gbps dla rozpoznawania i kontroli aplikacji,
  - b. Minimum 0.8 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,
  - c. Minimum 11.000 nowych sesji na sekundę,
  - d. Minimum 64.000 równoległych sesji.

Warunki serwisu technicznego i procedura zgłoszeń

4. Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.
5. Wsparcie techniczne musi być świadczone przez okres do 31.12.2026r.
6. W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.

**II. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA – 2 szt. serwer fizyczny;**

Nazwa elementu, parametru lub cechy	Opis wymagań Serwerów
<b>Obudowa</b>	Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
<b>Procesor</b>	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.2GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora nie powinien być niższy niż 286 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org ( <a href="http://www.spec.org">www.spec.org</a> ), dla serwera oferowanego producenta.
<b>Liczba zainstalowanych procesorów</b>	2
<b>Płyta główna</b>	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
<b>Pamięć operacyjna</b>	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w kościach 32GB Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
<b>Zabezpieczenie pamięci</b>	Memory mirroring, ECC, SDDC, ADDDC
<b>Procesor Graficzny</b>	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.

<b>Rozbudowa dysków</b>	<p>Zainstalowane z tyłu obudowy dwa dyski NVMe M.2 o pojemności minimum 960GB każdy zabezpieczone sprzętowym RAID 1. Dyski muszą mieć możliwość wymiany na gorąco.</p> <p>Wymagany jest wewnętrzny slot na kartę Micro SD.</p>
<b>Zasilacz</b>	Minimum dwa redundantne zasilacze o mocy minimum 800W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
<b>Interfejsy sieciowe</b>	<p>Zainstalowane dwuportowa karta 10GBASE-T. Karta nie może zajmować żadnego ze slotów PCIe.</p> <p>Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.</p>
<b>Sloty I/O</b>	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 x8 z czego jeden High-Profile, 2 sloty OCP Gen5 oraz jeden slot PCIe wewnątrz obudowy serwera dedykowany pod kontroler dyskowy.
<b>Dodatkowe porty</b>	<ul style="list-style-type: none"> <li>• z przodu obudowy: możliwość instalacji 2x USB 3 (z czego jeden z możliwością zarządzania serwerem) , zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu Mini DisplayPort</li> <li>• z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9.</li> <li>• wewnątrz obudowy: Możliwość instalacji portu USB 3 wewnątrz obudowy.</li> </ul> <p>Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA,, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płycie I/O, którą łączy się bezpośrednio z płytą główną serwera.</p>
<b>Chłodzenie</b>	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
<b>Zarządzanie</b>	<p>Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty).</p> <ul style="list-style-type: none"> <li>• Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna</li> <li>• Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja</li> </ul>

- 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.
- Wysyłanie 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 mediów z wykorzystaniem Java client
- Przekierowanie konsoli 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 kartą 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 serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.

Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:

- zarządzanie infrastrukturą serwerówi storage bez udziału dedykowanego agenta
- przedstawianie graficznej reprezentacji zarządzanych urządzeń
- możliwość skalowania do minimum 1000 urządzeń
- obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2
- wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych
- udostępnianie szybkiego podglądu stanu środowiska
- udostępnianie podsumowania stanu dla każdego urządzenia
- tworzenie alertów przy zmianie stanu urządzenia
- monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,
- konsola zarządzania oparta o HTML 5
- dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,
- automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja
- możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania
- definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń
- definiowanie ról użytkowników oprogramowania
- obsługa REST API oraz Windows PowerShell
- obsługa SNMP, SYSLOG, Email Forwarding



- autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML
- obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami
- przedstawianie historycznych aktywności użytkowników
- blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych
- tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv
- Obsługa NTP
- przesyłanie alertów do konsoli firm trzecich
- tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)
- instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie
- możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,

Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami:

VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.

#### Funkcje zabezpieczeń

Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. 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.

<b>Obsługa</b>	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
<b>Diagnostyka</b>	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID  Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu powinno odbywać się poprzez dedykowany port USB na froncie serwera. Wymaga się aby serwer posiadał diody sygnalizacyjne awaryjne przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
<b>Systemy operacyjne</b>	Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux 9.x; SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3; Ubuntu 22.04, 24.04
<b>Gwarancja</b>	36 miesięcy gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.

### III. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1x (switch) – 5 szt. switch typ I, 2 szt. switch typ II;

#### Switch typ I – 5 szt.

1. 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. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

2.1 możliwość montażu w stelażu/szafie 19"

2.2 wysokość maksymalna 1U

2.3 głębokość bez zainstalowanego zasilacza nie większa niż 35 cm

2.4 minimum jeden zasilacz 230V AC

2.5 zakres temperatur pracy ciągłej co najmniej od 0°C do +40 °C

2.6 zakres wilgotności pracy co najmniej 10% - 90%

3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:

3.1 24 porty RJ45 2.5Gbps

3.2 4 porty 10GE SFP+

3.3 Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.

4. Przełącznik musi posiadać następujące porty służące do zarządzania:

4.1 Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45

5. Układ przełączający o wydajności min. 200 Gbps, wydajność przełączania przynajmniej 148 Mpps

6. Obsługa min. 16 000 adresów MAC

7. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

8. Możliwość skonfigurowania min. 4000 interfejsów vlan

9. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

10. Obsługa minimum 8 grup LAG

11. Obsługa ramek jumbo o wielkości min. 9 KB

12. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).

13. Obsługa protokołów związanych z obsługą ruchu typu multicast:

13.1 IGMP Snooping v2 i v3

13.2 MLD Snooping

14. Minimalny rozmiar tablicy ARP 500 wpisów

15. Obsługa protokołów LLDP i LLDP-MED

16. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client

17. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

17.1 autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu

17.2 możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

17.3 zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2

17.4 możliwość synchronizacji czasu zgodnie z NTP lub SNTP

18. Implementacja co najmniej ośmiu kolejek QoS.

19. 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

20. Zamawiający wymaga, aby urządzenia posiadały serwis gwarancyjny świadczony przez Wykonawcę lub właściwy serwis producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD.

Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).

21. Usługa serwisu musi być świadczona w języku polskim.

22. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

### **Switch typ II – 2 szt.**

1. 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. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

2.1 możliwość montażu w stelażu/szafie 19"

2.2 wysokość maksymalna 1U

2.3 głębokość bez zainstalowanego zasilacza nie większa niż 35 cm

2.4 minimum jeden zasilacz 230V AC

2.5 zakres temperatur pracy ciągłej co najmniej od 0°C do +40 °C

2.6 zakres wilgotności pracy co najmniej 10% - 90%

3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:

3.1 16 portów 10GE SFP+

3.2 Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.

4. Przełącznik musi posiadać następujące porty służące do zarządzania:

4.1 Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45

5. Układ przełączający o wydajności min. 320 Gbps, wydajność przełączania przynajmniej 230 Mpps

6. Obsługa min. 16 000 adresów MAC

7. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

8. Możliwość skonfigurowania min. 120 interfejsów vlan

9. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

10. Obsługa minimum 8 grup LAG

11. Obsługa ramek jumbo o wielkości min. 9 KB

12. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).

13. Obsługa protokołów związanych z obsługą ruchu typu multicast:

13.1 IGMP Snooping v2 i v3

13.2 MLD Snooping

14. Minimalny rozmiar tablicy ARP 500 wpisów

15. Obsługa protokołów LLDP i LLDP-MED

16. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client

17. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

17.1 autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu

17.2 możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

17.3 zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2

17.4 możliwość synchronizacji czasu zgodnie z NTP lub SNTP

18. Implementacja co najmniej ośmiu kolejek QoS.

19. 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

20. Zamawiający wymaga, aby urządzenia posiadały serwis gwarancyjny świadczony przez Wykonawcę lub właściwy serwis producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).

21. Usługa serwisu musi być świadczona w języku polskim.

22. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

#### IV. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise – 6 szt.;

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	Access point
Częstotliwość	2,4 GHz 5 GHz
Maksymalna szybkość przesyłania danych	1770 Mbit/s
Maksymalna szybkość przesyłania danych (2.4 GHz)	570 Mbit/s
Maksymalna szybkość przesyłania danych (5 GHz)	1200 Mbit/s
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s



Standardy komunikacyjne	IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az
Automatyczne MDI/MDI-X	Tak
MIMO	Tak
Typ MIMO	Multi User MIMO
Metoda rozszerzenia obrazu	DSSS, OFDM, OFDMA
Modulacja	16-QAM, 64-QAM, 256-QAM, 1024-QAM, BPSK, CCK, QPSK
Szyfrowanie / bezpieczeństwo	WPA3, WPA, WPA2
Porty i interfejsy	Ethernet LAN (RJ-45) 1szt; USB 2.0 (USB typu A) 1szt.
Obsługa PoE	Tak
Maksymalne zużycie mocy	16,5 W
Zakres wilgotności względnej	5 - 93%
Zakres temperatur (eksploatacja)	0 - 50 °C
Zakres temperatur (przechowywanie)	-40 - 70 °C
Dopuszczalna wilgotność względna	5 - 93%

## V. Oprogramowanie / licencje NAC ( Network Access Control) – licencja obejmująca 150 urządzeń końcowych;

Podstawowa funkcjonalność systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 150 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 5 000

- jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
  9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
  10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
    - Maszyny fizyczne - serwery wspierane przez producenta.
  11. System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
  12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
  13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
  14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
  15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now.
  16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.

17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.

35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfigurację maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.

55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
  - Czy włączony jest firewall
  - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
  - Czy jest włączone szyfrowanie dysku systemowego
  - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
  - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
  - Czy w systemie są uruchomione procesy wskazane przez administratora
  - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
  - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
    - Wartości klucza rejestru
    - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfigurator sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
- Microsoft Windows
  - Mac OS
  - iOS
  - Android



63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

#### Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
  - MAC,
  - PAP/ASCII,
  - CHAP,
  - SNMP,
  - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
  - Tożsamość/Urządzenie końcowe,
  - Grupa tożsamości/urządzeń końcowych,
  - Parametry urządzeń końcowych, min: system operacyjny, wersja,
  - Atrybuty Active Directory,
  - Jednostka organizacyjna tożsamości/urządzeń końcowych,
  - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
  - Grupy urządzeń sieciowych,
  - Porty urządzeń sieciowych,
  - Grupy portów urządzeń sieciowych,
  - Jednostka organizacyjna portów,
  - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
  - Data, czas ważności polityki,

- Wewnętrzny Captive Portal,
  - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
  9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
  10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
  11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
  12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
  13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
  14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
  15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
  16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
  17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
  18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
  19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
  20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

#### Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:

- możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
- możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
- Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
- usługę OCSP (Online Certificate Status Protocol).

#### Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
  - Uruchamianie usługi dla wybranych podsieci,
  - Przypisanie ustalonego adresu IP dla adresu MAC.
  - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
  - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
  - Możliwość określania braku dostępu dla wybranych adresów MAC,
  - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
  - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
  - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
  - Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
  - Dokonywanie zmian bez konieczności wyłączania usług.

#### Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.

7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

#### Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:

- Logowania, wylogowania z system w tym błędne logowania
- Logowania do sieci 802.1X

#### Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
  - wiadomości e-mail,
  - Syslog,
  - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
  - Ilości obsługiwanych transakcji RADIUS,
  - Opóźnienie obsługi transakcji RADIUS,
  - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
  - badanie łączności IP za pomocą ping, traceroute,
  - tcpdump protokołów RADIUS, TACACS+,
  - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
    - nazwy użytkownika,
    - adresu MAC,
    - statusu uwierzytelnienia (udana lub nieudana),
    - powodu, jeżeli uwierzytelnienie nieudane,
    - zakresu czasowego, co do dnia, godziny i minuty,
  - wykonanie zdalnego polecenia na urządzeniu sieciowym.

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC –licencje na wsparcie producenta oprogramowania na okres do 31.12.2026r. Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązywania problemów związanych z wdrożeniem lub obsługą systemu NAC
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.



- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

## **VI. System operacyjny, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 2 szt. system operacyjny;**

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2016 Standard i wymagana dostarczenia licencji na oprogramowanie Microsoft Windows Server 2025 Standard lub nowszy lub równoważny serwerowy system operacyjny.

### **Opis równoważności oprogramowania**

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wszystkie elementy systemu oraz jego licencja pochodzą od tego samego producenta.
2. Wymaga się dostarczenia odpowiedniej liczby licencji dla serwerów, 2 i 1- procesorowych, posiadających min 12 rdzeni,
3. Jeżeli wymagane jest posiadanie licencji dostępowych, należy dostarczyć licencję dla odpowiedniej liczby użytkowników.
4. Licencja na SSO zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 2 w środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji.
5. SSO posiada graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.
6. Obsługa do 48 TB RAM
7. SSO musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP
8. Możliwość uruchomienia posiadanego, skonfigurowanego i używanego przez Zamawiającego oprogramowania do backupu, aktualnie zainstalowanego na systemie operacyjnym Windows.
9. Pełna współpraca z procesorami o architekturze 64 bit
10. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
11. SSO zapewniający natywne wsparcie dla środowiska .NET Framework 4.x
12. System operacyjny musi wspierać pracę domenową.
13. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory
14. Zawarta możliwość uruchomienia roli serwera DNS
15. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
16. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu.
17. Interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim,
18. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,

19. Możliwość dokonywania bezpłatnych aktualizacji i poprawek
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
21. Zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników,
22. Mechanizmy logowania w oparciu o login i hasło,
23. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT).
24. 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).
25. 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.
26. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
27. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
28. 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, udział sieciowy).
  - c. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych.
29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
31. Dostarczone oprogramowanie musi być fabrycznie nowe.

**VII. Licencje dostępowe do systemu, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – licencje dla 60 użytkowników;**

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2016 Standard i w pkt. VII. wymagana dostarczenia licencji na oprogramowanie Microsoft Windows Server 2025 Standard lub nowszy lub równoważny serwerowy system operacyjny.

W ramach zamówienia Zamawiający wymaga dostarczenia licencji dostępowych CAL User dla 60 użytkowników lub równoważne licencje dostępne dla oferowanego, równoważnego systemu operacyjnego.

### **VIII. Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowane siecion OT – 1 szt. licencji;**

Przedmiotem zamówienia jest:

1. wdrożenie systemu monitorowania sieci przemysłowej służącym do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2. dostawa licencji oraz sond sprzętowych,
3. udzielenie wsparcia dla administratorów Zamawiającego,
4. organizacja i realizacja szkoleń dla administratorów Zamawiającego.

Funkcjonalność i specyfikacja.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. sondy sprzętowe oraz oprogramowanie muszą pochodzić od tego samego producenta.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:
  - a. pasywne monitorowanie sieci przemysłowej Zamawiającego,
  - b. automatyczne tworzenie graficznej mapy rządu min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
  - c. szczegółową inwentaryzację urządzeń,

- d. automatyczne odzwierciedlenie połączeń komunikacyjnych,
  - e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
  - f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
  - g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
  - h. obsługę LLDP, CDP, CIP, SSDP.
10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
  11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
  12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
  13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
  14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line” przy wpięciu do linii.
  15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
  16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
  17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
  18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
  19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)
  20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
  21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
  22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
  23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
  24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
  25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.
  26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.

27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:
  - a. malware/"zero-day",
  - b. atak DOS/DDOS,
  - c. atak typu ATP,
  - d. spyware, skanowanie sieci,
  - e. zagrożenia Man-in-the-Middle,
  - f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
  - g. wykrywanie połączeń do innej sieci LAN/internet,
  - h. wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.
29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BROADCAST.
34. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.
35. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
36. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
37. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
38. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
39. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
40. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
41. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem baterijnym do 30 minut przy zaniku zasilania z sieci.
42. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
43. Sonda sprzętowa musi być zabezpieczona przed ingerencją tzn.: dane muszą zostać skasowane przy próbie odczytu pamięci FLASH.
44. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
45. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.



46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
49. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
50. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
51. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

Dostawa, wdrożenie.

1. Wykonawca dostarczy:
  - a. sondy sprzętowe w liczbie 2 szt. do monitorowania sieci przemysłowej,
  - b. licencję na oprogramowanie dla nielimitowanej liczby monitorowanych urządzeń,
  - c. licencję wieczystą na system IDS oraz serwis (utrzymanie i eksploatacja urządzeń, wsparcie) producenta systemu IDS na okres do 31.12.2026r.

Serwis producenta systemu IDS ma obejmować:

- Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
  - Dostęp do nowych wersji systemu IDS.
  - Dostęp do aktualizacji i poprawek systemu IDS.
  - Dostęp do aktualizacji oprogramowania sond sprzętowych.
  - Wymianę uszkodzonych sond sprzętowych w razie awarii.
  - Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
  - Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
  - Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
2. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku wirtualnym będącym częścią zamówienia.
  3. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
  4. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.

5. Wykonawca prześle Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
6. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.

## **IX. Oprogramowanie SIEM (Security Information and Event Management) – 1 szt. licencji;**

### **Wymagania funkcjonalne**

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu.
6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
7. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie
8. System musi zapewniać retencję danych w okresie minimum 365 dni.
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
14. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregośkolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
18. Interfejs musi posiadać angielską lub polską wersję językową.

19. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
23. System musi wspierać mechanizm logowania typu Single Sign On.
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
26. System powinien umożliwiać zarządzanie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historii operacji, realizowanych zapytań, zmian uprawnień.
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
31. System musi pozwalać na tworzenie parserów z poziomu GUI
32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
37. System musi zapewniać parsowanie wpływających do niego wiadomości w formatach:
  - Syslog,
  - WEF,

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

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

38. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
39. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
40. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
41. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
42. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
43. System musi posiadać predefiniowany zestaw parserów zdarzeń.
44. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
45. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
46. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
47. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
48. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
49. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.

50. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
51. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
52. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
53. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
54. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
55. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
56. Wykrycia dowolnej treści w logach,
57. Wykrycia wystąpienia wartości pola na wybranej liście,
58. Wykrycia niewystępowania wartości pola na wybranej liście,
59. Wykrycia zmiany jednego z kilku pól,
60. Wykrycia zdarzeń występujących z zadaną częstotliwością,
61. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
62. Wykrycia zaniku Wiadoomości,
63. Wykrycia nowej wartości pola w zadanym okresie,
64. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
65. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
66. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
67. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
68. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
69. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
70. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
71. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
72. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.



73. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
74. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
75. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
76. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
77. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
78. System umożliwia konfigurację automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
79. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
80. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
81. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
82. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
83. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres do 31.12.2026r.
84. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
85. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
86. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
87. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
88. System musi umożliwiać integrację z Mitre ATT@CK.

#### Reguły korelacyjne, alerty i obsługa incydentów

89. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
90. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów,

zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.

91. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
92. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
93. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
94. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
95. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP

#### Wymagania funkcjonalne dla sytemu SOAR

1. Oprogramowanie musi wspomagać pracę zespołu reagowania na incydenty komputerowe (SOC, CERT, CSIRT, IRT itp.) tj. wspomagać procesy: monitorowania bezpieczeństwa teleinformatycznego, reagowania na incydenty, zarządzania podatnościami, gdzie głównym celem jest standaryzacja i automatyzacja działań analityków cyberbezpieczeństwa.
2. Oprogramowanie musi natywnie integrować się z systemem klasy SIEM wykorzystywanym przez Zamawiającego tj. producent oprogramowania SOAR musi oficjalnie wspierać integrację z dostarczonym rozwiązaniem SIEM.
3. Oprogramowanie musi umożliwiać automatyczne tworzenie incydentów wymagających obsłużenia na podstawie powiadomień z systemu klasy SIEM, zgłoszeń przekazywanych przez użytkowników na dedykowany adres e-mail, zgłoszeń przypisanych w systemie typu helpdesk do odpowiedniej grupy, przez co najmniej system RTIR (Request Tracker Incident Response) lub Jira. Ponadto rozwiązanie musi umożliwiać automatyczne zamykanie obsłużonego zgłoszenia w systemie typu helpdesk, przynajmniej dla rozwiązania RTIR (Request Tracker Incident Response) lub Jira.
4. Oprogramowanie musi umożliwiać ręczne utworzenie incyduentu.
5. Oprogramowanie musi posiadać możliwość automatycznej oraz ręcznej klasyfikacji incydentów ze względu na ich krytyczność.
6. Oprogramowanie musi umożliwiać tworzenie własnych definicji klasyfikacji incydentów i ich krytyczności. W ramach wdrożenia Wykonawca wraz z zamawiającym ustali oraz zaimplementuje właściwą klasyfikację incydentów w systemie.
7. Oprogramowanie musi umożliwiać śledzenie czasu oraz podjętych działań w ramach utworzonego incyduentu oraz raportowanie czasów: Time-to-detect oraz czasów: Time-to-mitigate.
8. Oprogramowanie musi umożliwiać łączenie utworzonych incydentów, w tym inteligentne łączenie automatyczne.
9. Oprogramowanie musi umożliwiać automatyczne przydzielanie predefiniowanych zadań dla danych typów incydentów.

10. Oprogramowanie musi umożliwiać tworzenie i edytowanie procedur reagowania na incydenty w postaci graficznej. System musi umożliwiać stosowanie podstawowych operatorów logicznych i matematycznych przy definicji procedur.
11. Oprogramowanie musi umożliwiać automatyczne oraz ręczne przydzielanie incydentów wymagających obsłużenia do pracowników obsługujących system.
12. Oprogramowanie musi umożliwiać automatyczną oraz ręczną weryfikację w wewnętrznych oraz zewnętrznych źródłach informacji, charakterystycznych dla danego incydentów atrybutów.
13. Oprogramowanie musi umożliwiać zaprojektowanie oraz wdrożenie automatycznych działań reagowania na dane typy incydentów.
14. Oprogramowanie musi umożliwiać edycję kodu źródłowego automatycznych działań reagowania. Wymaga się stosowanie języka skryptowego uznanego za powszechny, w jego najnowszej wersji. Np. Python3.
15. Oprogramowanie musi umożliwiać tworzenie zbiorczych raportów z utworzonych oraz obsłużonych incydentów.
16. Oprogramowanie musi integrować się przynajmniej z następującymi systemami Zamawiającego:
  - Office 365 / Microsoft Exchange (pobranie lub wysłanie maili)
  - Slack (wysyłka komunikatów)
  - Energy Logserver
17. Oprogramowanie musi umożliwiać łatwą integrację z pozostałymi systemami klasy threat intel/threat hunting/threat share za pomocą API.
18. System musi posiadać możliwość generowania dashboardów security z danych znajdujących się w SOAR, między innymi statystyk, w tym system musi posiadać możliwość tworzenia i konfiguracji widoków głównych na główny ekran dyspozycyjny w pomieszczeniu SOC.
19. Umożliwiać dwustronną komunikację z użytkownikami systemu (np. w celu zebrania dodatkowych informacji od osób związanych z incydemtem) oraz operatorami systemu SOAR, na przykład poprzez zastosowanie interaktywnych formularzy.
20. Zapewniać zestaw co najmniej 250 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.
21. Automatyzować proces analizy otrzymanych danych, realizować funkcje informacyjne, jak również podejmować funkcje naprawcze (np. automatyczna analiza pliku w chmurze sandbox wybranego producenta, wysłanie wiadomości e-mail do użytkownika zainfekowanej stacji końcowej, aby nie otwierał załącznika i blokada na urządzeniu sieciowym dostępu do wskazanych usług dla wybranego użytkownika).
22. Posiadać wbudowaną bibliotekę minimum 5 typów incydentów, a także powinno dostarczać specjalizowane typy incydentów związane z integrowanymi systemami, pozwalając jednocześnie na ich edycję lub kopiowanie celem stworzenia własnej karty incydemtu.

23. Umożliwić wykorzystanie w skryptach własnych bibliotek zewnętrznych oraz programów (np. poprzez umożliwienie uruchomienia skryptów we własnym kontenerze, zawierającym pożądane oprogramowanie).
24. Zapewniać możliwość wglądu w kod integracji oraz jego klonowanie pod kątem wprowadzania modyfikacji lub napisania własnej wersji integracji.
25. Pozwalać na kopiowanie oraz edycję już istniejących scenariuszy jak również dodawanie nowych.
26. Pozwalać na edycję i dodawanie nowych scenariuszy obsługi incydentu (tzw. playbook) za pomocą graficznego interfejsu użytkownika bez konieczności wykorzystania języków skryptowych lub znajomości języków programowania.
27. Pozwalać na tworzenie scenariuszy zagnieżdżonych, tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane na zasadzie pod-scenariuszy. Edycja/zmiana pod-scenariusza wpływa automatycznie na wszystkie scenariusze, które go wykorzystują, co ułatwia administrację.
28. Pozwalać na tworzenie scenariuszy zawierających:
  - zadania ręczne
  - zadania zautomatyzowane
  - zadania warunkowe automatyczne
  - zadania warunkowe ręczne
  - akwizycję danych przy użyciu formularzy
  - filtry danych
  - pod-scenariusze.
29. Pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy.
30. Pozwalać na automatyczne dokumentowanie uruchomionych scenariuszy wraz z wynikami jego działania
31. Umożliwiać wizualizacje przebiegu wykonania scenariusza (wizualizacje rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.).
32. Pozwalać na sterowanie wykonaniem scenariusza przez operatora (zadania warunkowe ręczne) drogą korespondencyjną (m.in. z poziomu wiadomości email oraz wiadomości w komunikatorze takim jak np. Microsoft Teams, Slack, Mattermost itp.).
33. Pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów.
34. Pozwalać na ponowne uruchomienie scenariusza na konkretnym incydencie, jeżeli zajdzie taka potrzeba.
35. Pozwalać na zatrzymanie scenariusza w trakcie jego wykonania.
36. Pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń).

37. Pozwalać na proste monitorowanie stanu wykonania scenariuszy powiązanych z incydentami. Ponadto, w przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza, osoby odpowiedzialne za incydent powinny zostać natychmiast o tym poinformowane.
38. Pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.
39. Pozwalać na przekazywanie parametrów pomiędzy zadaniami pojedynczego scenariusza.
40. Pozwalać na odczytywanie wyników analizy i wykorzystaniu ich w kolejnych zadaniach uruchomionego scenariusza.
41. Pozwalać na sprawdzenie historycznych danych na temat uruchomionych scenariuszy/zadań.
42. Pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i wedle harmonogramu.
43. Pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.
44. Pozwalać na tworzenie własnych:
  - Typów incydentów
  - Pól/etykiet incydentów
  - Typów wskaźników (ang. indicator)
  - Pól/etykiet wskaźników (ang. indicator)
  - Raportów
  - Dashboardów.
45. Pozwalać na automatyczne wypełnianie pól incydentu bazując na typie incydentu lub jego atrybutach.
46. Pozwalać na delegowanie zadań innym członkom zespołu SOC w ramach oceny danego incydentu.
47. Pozwalać na współpracę pomiędzy członkami zespołu SOC (np. rozmowa między członkami zespołu a temat incydentu).
48. Pozwalać na zapisywanie historycznych incydentów wraz z pełną informacją na temat podjętych akcji obsługi/rozwiązania w celu szkolenia/transferu wiedzy pomiędzy członkami zespołu SOC (Na historię incydentu składają się wyniki działania automatycznych i ręcznych zadań określonych w playbooku, komentarze analityków pracujących nad incydentem, indykatory zagrożenia IOC (IP, URL, domeny, itd.) wyciągane automatycznie i wskazywane ręcznie w czasie obsługi incydentu, elementy analizy oznaczone przez analityków jako dowód w sprawie (np. zrzuty ekranu z widokiem podejrzanych stron web), pliki dodawane do historii obsługi incydentu przez analityków, itp.).
49. Pozwalać na export wskaźników kompromitacji do serwerów MISP.
50. Pozwalać na import zdarzeń z serwerów MISP.
51. Pozwalać na eksport incydentów w formatach STIX 1/2, CSV, PDF.



52. Pozwalać na tworzenie wielu instancji integracji tego samego typu do rozwiązań firm trzecich (przykładowo dwie integracje z serwerami IMAP lub zaczytujące dane threat intel z dwóch źródeł w formacie JSON).
53. Pozwalać na rozszerzenie możliwości systemu w zakresie tworzenia i edycji scenariuszy poprzez dodanie własnych skryptów realizujących niestandardową logikę operacji warunkowych, filtracji danych, modyfikacji danych, a także skryptów realizujących niestandardową prezentację danych w dashboardach, zadania wykonywane po zakończeniu obsługi incydentu itp.
54. Pozwalać na proste wprowadzenie globalnych zestawów poświadczeń w celu ułatwienia użycia wspólnego konta technicznego w wielu integracjach z systemami trzecimi.
55. Posiadać zestaw przygotowanych raportów takich jak:
56. Raport na temat incydentów: dzienny, 7- i 30-dniowy
57. Raport na temat średniego czasu rozwiązania incydentu
58. Pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację pożądaných danych (np. wykres kołowy, słupkowy, liniowy, tabela itp.).
59. Pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego języka zapytań) oraz podobieństwa do innych incydentów (related incidents).
60. Pozwalać na wizualizację zależności pomiędzy podobnymi incydentami na poziomie wystąpień identycznych indykatorów.
61. Pozwalać na eksport raportów w formacie, co najmniej PDF.
62. Mieć możliwość działania jako platforma SOAR dla wielu instytucji/klientów z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant).
63. Posiadać repozytorium wskaźników (ang. indicators), które kolekcjonuje i koreluje wskaźniki w ramach wszystkich incydentów, alertów i feedów dostarczanych do rozwiązania.
64. Posiadać możliwość wykonywania scenariuszy na podstawie zestawu wskaźników (ang. indicators) określonych przez użytkownika.
65. Być w stanie obsługiwać formaty strukturalne, takie jak JSON, CSV, STIX 1.X i STIX 2.X itp. w ramach integracji ze źródłami wskaźników (ang. indicators).
66. Wspierać minimum następujące typy wskaźników (ang. indicators):
  - numery kart płatniczych
  - IBAN
  - adres email
  - konto użytkownika
  - wyniki CVE
  - domena
  - FQDN
  - nazwy hosta

- IP (v4 oraz v6)
- klucz i ścieżka rejestru
- URL
- CIDR.

67. Umożliwiać własną definicję wskaźników, jego pól oraz skryptów reputacyjnych.
68. Zapewniać użytkownikom możliwość automatycznej weryfikacji wskaźników (tzw. enrichment), wykonując odpowiedni scenariusz lub uruchamiając sprawdzanie na podstawie typu wskaźnika (ang. indicator).
69. System musi posiadać natywną integrację z MITRE ATT&CK i przypisywać do incydentów odpowiednie techniki i taktyki
70. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres do 31.12.2026r.

#### X. Network Attached Storage (NAS) – 2 szt. NAS;

Poniżej przedstawiono minimalne wymagania dla 1 sztuki macierzy. Zamawiający oczekuje dostawy 2 sztuk macierzy o parametrach nie niższych niż poniższe:

Procesor	Wielordzeniowy procesor o architekturze 64-bitowej osiągający minimum 4 tysiące punktów w teście PassMark.		
Obudowa	Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie.		
Pamięć RAM	Minimum 4GB DDR4 ECC. Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników.		
Ilość obsługiwanych dysków	Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 20TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków.		
Zainstalowane dyski	8 dysków o pojemności 12TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1 milion, - możliwość aktualizacji oprogramowania dysku bezpośrednio z poziomu systemu operacyjnego serwera NAS.		
Interfejsy sieciowe	Minimum 4 porty 10GbE RJ-45.  Obsługa agregacji łączy.	1GbE	RJ-45.

Porty	Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.
Wskaźniki LED	Status, HDD, zasilanie, LAN
Obsługa RAID	Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP
Usługi	<p>1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer plików, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.</p> <p>2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 10 i 11 według harmonogramu z możliwością zarządzania tworzeniem zadań kopii zapasowych z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.</p> <p>3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.</p>
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	Minimum 36 miesięcy gwarancji.
Waga bez dysków	Maksymalnie 15 kg
Typowy pobór mocy podczas pracy	Maksymalnie 130W
Certyfikaty	CE
System plików	Dyski wewnętrzne: BTRFS

Szyfrowanie	Mechanizm szyfrowania sprzętowego
Zasilacz	Redundantny zasilacz o mocy minimum 300W.
Chłodzenie	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej.

**XI. System wirtualizacyjny dedykowany do systemów, na których zostanie zainstalowany produkt z zakresu cyberbezpieczeństwa – 1 szt. licencji;**

LP.	Wymagania funkcjonalno-techniczne (minimalne)
1	Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera
2	Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
3	Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
4	Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 320 logicznych wątków oraz do 4TB pamięci fizycznej RAM.
5	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych.
6	Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB
7	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
8	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych.
9	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 2 porty szeregowo.
10	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.

11	Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12	Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade).
13	Rozwiązanie musi umożliwiać poprawne zainstalowanie następujących systemów operacyjnych: Windows Server 2019, Windows Server 2022, Windows Server 2025, Windows 7, Windows 8, Windows 10, SLES 11, SLES 10, RHEL 6, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 12.04
14	Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15	Rozwiązanie powinno posiadać centralną konsolę do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
16	Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
17	Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
18	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
19	Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
20	Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych.
21	Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.



22	Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
23	System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.
24	Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
25	Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
26	Należy dostarczyć licencję obsługującą 2 serwery po 2 procesory tak, aby licencja pozwalała na pełne wykorzystanie serwerów z pkt. III.

## **XII. Serwer do wykonywania kopii zapasowych – 1 szt. serwera do backupu;**

### Zarządzanie i magazyny

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025 r.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
  - a. Obudowa rack rozmiar: 1U
  - b. Procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora 2.6GHz
  - c. Pamięć RAM: 16GB
  - d. Przestrzeń dostępna na przechowywanie danych:  
Min. 24 TB po RAID 5
  - e. Osobne dyski SSD M.2 NVMe działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
  - f. Redundantne zasilanie,
  - g. Interfejsy sieciowe:  
Min. 2szt. Ethernet 1Gb, Dual SFP28
  - h. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.

4. Produkt dostępny w polskiej wersji językowej.
5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
8. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
9. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
10. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
11. System zarządzania nie może być oparty o relacyjne bazy danych.
12. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
13. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
14. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
15. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie.
16. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
19. Rozwiązanie zapewnia backup jednorzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.

23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
29. Rozwiązanie musi być skalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.

38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie danych.
45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
52. System powinien posiadać predefiniowane schematy tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, S3, nfs, iscsi, katalog lokalny

56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
58. Możliwość generowania raportów dobowych w oparciu o harmonogram
59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienie e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

#### Wspierane systemy

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

Alpine 3.10+,  
Debian: 9+,  
Ubuntu: 16.04+,  
Fedora: 29+,  
centOS: 7+,  
RHEL: 6+,  
openSUSE: 15+,  
SUSE Enterprise Linux(SLES): 12 SP2+,  
macOS: 10.13+,  
Windows: 7, 8.1, 10(1607+), 11+  
Windows Server: 2008 R2+,

#### Środowisk wirtualnych:

Hyper-V 2016+,  
VMware: 6.7+.



## Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

## Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.

2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdedykowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

#### Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

#### Licencjonowanie i wsparcie techniczne

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

2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta w okresie do 31.12.2026r.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Wsparcie techniczne musi być świadczone w modelu 24/7.
5. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
6. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
7. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
8. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.

#### Anty-ransomware i bezpieczeństwo

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

### **XIII. Usługa kopii zapasowych w chmurze obliczeniowej IT/OT/ICS – licencja na usługę kopii zapasowych w chmurze obliczeniowej min. 4TB;**

#### Ogólne

1. Rozwiązanie musi umożliwiać tworzenie wielu repozytoriów danych na innych środowiskach jako przestrzeń do replikacji danych.
2. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych.

3. Rozwiązanie musi być dostarczone w postaci paczki przestrzeni o pojemności 4 TB.

#### Magazyny chmurowe

1. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
2. Produkt musi posiadać możliwość replikacji kopii zapasowych z urządzenia do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
3. Produkt musi posiadać możliwość replikowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
4. Produkt musi posiadać możliwość replikacji kopii zapasowych między dwoma magazynami chmurowymi Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.

#### Proces replikacji

5. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
6. System pozwala na ustawienie jednego lub wielu zadań replikacji, pozwalając odmiejszcwić kopię w kilku lokalizacjach jednocześnie.

#### Przywracanie danych odmiejszczonych

7. Odzyskiwanie danych z kopii może odbywać się bezpośrednio z magazynu replikacyjnego do urządzenia docelowego.
8. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia danych odmiejszczonych za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. odmiejszczone archiwum musi zawierać wszystkie informacje konieczne do odzyskania.

#### **XIV. Oprogramowanie do monitorowania infrastruktury informatycznej – 1 szt. licencji;**

1. Przedmiotem zamówienia jest zakup i dostawa licencji wieczystej dla 30 stacji roboczych.
2. Wsparcie techniczne wraz ze wszystkimi aktualizacjami, włącznie z przechodzeniem na wyższe wersję numeryczne na okres do 31.12.2026r.
3. Parametry podane w tabeli stanowią minimalne wymagania graniczne.

1.	Oprogramowanie:	<ol style="list-style-type: none"> <li>1. Budowa modułowa,</li> <li>2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2.</li> <li>3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.</li> </ol>
----	-----------------	--

		<p>4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych</p> <p>5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania</p>
2.	Monitorowanie danych użytkownika:	<p>1. historia aktywności</p> <p>2. polityka korzystania z Internetu i aplikacji</p> <p>3. dostęp do zewnętrznych nośników danych,</p> <p>4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodnie z RODO bez konieczności usunięcia informacji o stacji roboczej,</p> <p>5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO,</p> <p>6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników,</p> <p>7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia,</p> <p>8. konfiguracja haseł użytkownika</p> <p>9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej</p>
3.	Funkcjonalności:	<p>Oprogramowanie obsługuje m.in. 6 funkcjonalności:</p> <p>1. Monitorowanie infrastruktury,</p> <p>2. Inwentaryzacja sprzętu i oprogramowania,</p> <p>3. Monitorowanie aktywności użytkowników,</p> <p>4. Realizacja zdalnej pomocy użytkownikom,</p> <p>5. Ochrona danych przed wyciekiem,</p> <p>6. Wsparcie zarządzania czasem i analizowanie aktywności użytkowników</p>
4.	Monitorowanie infrastruktury:	<p>1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping,</p> <p>2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającą korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją,</p> <p>3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów.</p>



		<p>Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów,</p> <p>4. Serwery pocztowe:</p> <ul style="list-style-type: none"> <li>✓ program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty,</li> <li>✓ program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie,</li> <li>✓ program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa</li> </ul> <p>5. Monitorowanie serwerów WWW i adresów URL</p> <p>6. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS</p> <p>7. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail</p> <p>8. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID</p> <p>9. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych</p> <p>10. Monitoringu routerów i przełączników wg:</p> <ul style="list-style-type: none"> <li>✓ zmian stanu interfejsów sieciowych</li> <li>✓ ruchu sieciowego</li> <li>✓ podłączonych stacji roboczych – graficzna prezentacja panelu switcha</li> <li>✓ ruchu generowanego przez podłączone do portów stacje robocze</li> </ul> <p>11. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie,</p> <p>12. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu</p> <p>13. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano</p>
--	--	--

		<p>14. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny</p> <p>15. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy,</p> <p>16. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera.</p> <p>17. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.</p> <p>18. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia.</p> <p>19. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0</p>
5.	Inwentaryzacja sprzętu i oprogramowania,	<p>1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów,</p> <p>2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.</p> <p>3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.</p> <p>4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu</p> <p>5. Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.</p> <p>6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiegokolwiek zmiany na urządzeniu</p> <p>7. Możliwość odczytania numeru seryjnego (klucze licencyjne).</p> <p>8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.</p>

		<p>9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.</p> <p>10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).</p> <p>11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.</p> <p><i>Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:</i></p> <p>12. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,</p> <p>13. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,</p> <p>14. tworzenia powiązań między zasobami a urządzeniami,</p> <p>15. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory ), wskazywanie osób odpowiedzialnych,</p> <p>16. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,</p> <p>17. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości,</p> <p>18. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,</p> <p>19. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,</p> <p>20. masową edycję atrybutów zasobów,</p> <p>21. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,</p> <p>22. importu danych z zewnętrznego źródła (.CSV),</p> <p>23. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,</p>
--	--	--

		<p>24. tworzenia powiązań między zasobami a dokumentami w relacji 1:N,</p> <p>25. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutilizowany itp.,</p> <p>26. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,</p> <p>27. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,</p> <p>28. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,</p> <p>29. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,</p> <p>30. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,</p> <p>31. archiwizacji i porównywania audytów zasobów,</p> <p>32. tworzenia kodów kreskowych dla zasobów,</p> <p>33. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,</p> <p>34. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,</p> <p>35. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,</p> <p>36. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),</p> <p>37. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencja/gwarancja”).</p> <p><i>Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:</i></p>
--	--	---

		<ol style="list-style-type: none"> <li>1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.</li> <li>2. Informacje o aplikacjach używanych w organizacji.</li> <li>3. Tworzenie własnych wzorców aplikacji.</li> <li>4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.</li> <li>5. Informacje o komputerach, na których aplikacja została wykryta.</li> <li>6. Zarządzanie posiadanymi licencjami.</li> <li>7. Wskazywanie osób odpowiedzialnych za licencję.</li> <li>8. Wskazanie użytkowników licencji,</li> <li>9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.</li> <li>10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.</li> </ol>
6.	Monitorowanie aktywności użytkowników:	<ol style="list-style-type: none"> <li>1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),</li> <li>2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach,</li> <li>3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,</li> <li>4. Informacja o edytowanych przez użytkownika dokumentach,</li> <li>5. Historia pracy (cykliczne zrzuty ekranowe),</li> <li>6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),</li> <li>7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),</li> <li>8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość</li> </ol>



		<p>"grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków,</p> <p>9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail.</p> <p>10. Wykrywanie podejrzanej aktywności przez popularne „jigglerzy”, mającej na celu symulowanie faktycznej pracy.</p> <p>11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.</p> <p>12. Wyszczególnienie podejrzanej aktywności w raportach.</p> <p>13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności.</p> <p>14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.</p> <p>15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl).</p> <p>16. Blokowania ruchu na wskazanych portach TCP/IP,</p> <p>17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,</p> <p>18. Prowadzenie rejestru naruszeń blokad,</p> <p>19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,</p> <p>20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),</p> <p>21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.</p>
7.	Realizacja zdalnej pomocy użytkownikom	<p>1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika,</p>

		<p>2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów.</p> <p>3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów.</p> <p>Czat powinien pozwalać na:</p> <p>4. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej</p> <p>5. rozmowy między „zwykłymi” użytkownikami</p> <p>6. przesyłanie plików między rozmówcami w trybie online</p> <p>7. tworzenie pokoi tematycznych, rozmów grupowych</p> <p>8. oznaczanie kontaktów jako „ulubionych” na liście kontaktów</p> <p>9. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW helpdesku,</p> <p>10. Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów.</p> <p>Moduł pomocy zdalnej powinien umożliwiać:</p> <p>11. pobieranie listy użytkowników z Active Directory,</p> <p>12. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,</p> <p>13. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,</p> <p>14. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń,</p> <p>15. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,</p> <p>16. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,</p> <p>17. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,</p>
--	--	--

		<p>18. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,</p> <p>19. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,</p> <p>20. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,</p> <p>21. procesowanie zgłoszeń użytkowników z wiadomości e-mail,</p> <p>22. eksportowania listy zgłoszeń do plików CSV i XLSX,</p> <p>23. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,</p> <p>24. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,</p> <p>25. wykonywanie operacji na wielu zgłoszeniach równocześnie,</p> <p>26. dołączanie załączników do zgłoszeń,</p> <p>27. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,</p> <p>28. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,</p> <p>29. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,</p> <p>30. zrzuty ekranowe (podgląd pulpitu),</p> <p>31. zdalną modyfikację rejestrów,</p> <p>32. dystrybucję oprogramowania przez Agenty,</p> <p>33. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),</p> <p>34. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,</p> <p>35. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,</p> <p>36. planowanie nieobecności pracowników helpdesk,</p> <p>37. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,</p> <p>38. generowanie raportów obsługi helpdesk,</p>
--	--	--

		<p>39. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),</p> <p>40. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),</p> <p>41. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.</p>
8.	Ochrona danych przed wyciekiem	<p>Blokowanie urządzeń i nośników danych:</p> <ol style="list-style-type: none"> <li>1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.</li> <li>2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskiety.</li> <li>3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.</li> <li>4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezauważalnych.</li> <li>5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.</li> <li>6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.</li> <li>7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.</li> <li>8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.</li> <li>9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.</li> <li>10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender</li> <li>11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.</li> </ol>

		<p>Zarządzanie prawami dostępu do urządzeń:</p> <ol style="list-style-type: none"> <li>1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.</li> <li>2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp.</li> <li>3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.</li> <li>4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.</li> <li>5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.</li> </ol> <p>Audyt operacji na plikach na urządzeniach przenośnych:</p> <ol style="list-style-type: none"> <li>1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.</li> <li>2. Podłączenie/odłączenie urządzenia przenośnego.</li> <li>3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.</li> <li>4. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.</li> </ol>
9.	Zarządzanie czasem i analizowanie aktywności użytkowników	<ol style="list-style-type: none"> <li>1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym.</li> <li>2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje.</li> <li>3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.</li> </ol> <p>Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym.</p> <ol style="list-style-type: none"> <li>4. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.</li> <li>5. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.</li> </ol>



		<ol style="list-style-type: none"> <li>6. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.</li> <li>7. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.</li> <li>8. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.</li> <li>9. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.</li> <li>10. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.</li> <li>11. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).</li> <li>12. Wskaźnik czasu poświęconego na aktywność produktywną.</li> <li>13. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.</li> <li>14. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji.</li> <li>15. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.</li> </ol>
10.	Gwarancja, wsparcie serwisowe	<ol style="list-style-type: none"> <li>1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru</li> <li>2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania.</li> <li>3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania</li> <li>4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów).</li> <li>5. Świadczenie przez Producenta pomocy w formie sesji zdalnych.</li> </ol>

		<ul style="list-style-type: none"><li>6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy.</li><li>7. Możliwość przedłużenia wsparcia o kolejny rok</li><li>8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły</li></ul>
--	--	---

#### **XV. Wdrożenie oprogramowania z zakresu bezpieczeństwa – wdrożenie systemu typu opensource do analizy powłamaniowej;**

Przedmiotem zamówienia jest wdrożenie, konfiguracja bezpłatnego narzędzia typu Open Source przeznaczonego do informatyki śledczej (Digital Forensics), umożliwiającego analizę danych cyfrowych na potrzeby postępowań dowodowych, audytów lub kontroli wewnętrznych.

Wymagania ogólne dotyczące oprogramowania

1. Oprogramowanie musi być dostępne na licencji open source, umożliwiającej jego bezpłatne użytkowanie, modyfikowanie i dystrybucję.
2. Oprogramowanie musi działać na systemach operacyjnych typu Windows lub Linux.
3. Rozwiązanie musi zapewniać możliwość rozszerzania funkcjonalności poprzez moduły lub wtyczki.
4. Narzędzie musi umożliwiać analizę danych zarówno z nośników fizycznych, jak i z obrazów dysków.
5. Oprogramowanie nie może wymagać żadnych dodatkowych opłat licencyjnych.

Funkcjonalności wymagane

Oprogramowanie musi zapewniać co najmniej następujące funkcjonalności:

##### **1. Obsługa obrazów danych**

- 1) Wczytywanie popularnych formatów obrazów dysków i partycji (m.in. E01, Ex01, AFF, RAW/dd).
- 2) Obsługa obrazów urządzeń mobilnych i kopii logicznych (w miarę dostępności w narzędziu open source).

##### **2. Analiza systemów plików**

- 1) Analiza systemów plików m.in. NTFS, FAT, exFAT, EXT, HFS+, APFS.
- 2) Przeglądanie katalogów, metadanych, atrybutów plików.
- 3) Wyszukiwanie usuniętych plików i katalogów.

##### **3. Zaawansowane wyszukiwanie i indeksacja**

- 1) Automatyczna indeksacja zawartości plików.
- 2) Wyszukiwanie słów kluczowych także w plikach zagnieżdżonych (archiwa, dokumenty).
- 3) Obsługa wyrażeń regularnych.

##### **4. Analiza artefaktów systemowych**

Oprogramowanie musi posiadać moduły umożliwiające analizę m.in.:

- 1) historii przeglądarek internetowych,
- 2) plików dzienników systemowych,
- 3) rejestru systemowego,
- 4) list ostatnio otwieranych plików,
- 5) konfiguracji systemowych i użytkownika,
- 6) historii połączeń sieciowych.

5. Analiza danych multimedialnych

- 1) Przeglądanie obrazów, video, audio.
- 2) Wykrywanie plików o określonych sygnaturach (file carving).
- 3) Rozpoznawanie metadanych (EXIF i inne).

6. Raportowanie

- 1) Generowanie raportów w formatach PDF/HTML/CSV.
- 2) Możliwość tworzenia zestawień i eksportowania wyników analizy.
- 3) Oznaczanie znalezionych artefaktów jako dowody.

7. Praca z wieloma przypadkami

- 1) Tworzenie wielu projektów dochodzeniowych.
- 2) Oddzielne przechowywanie wyników analizy.
- 3) Eksport i import projektów.

Zakres wdrożenia

Wykonawca zobowiązany jest do:

- 1) Instalacji narzędzia na wskazanych stanowiskach Zamawiającego.
- 2) Konfiguracji oprogramowania zgodnie z potrzebami Zamawiającego.
- 3) Przeprowadzenia testów poprawności działania.

Wymagania dotyczące bezpieczeństwa

- 1) Oprogramowanie nie może wysyłać danych do zewnętrznych usług chmurowych.
- 2) Wszystkie dane dowodowe muszą być przetwarzane lokalnie.
- 3) Narzędzie musi umożliwiać pracę w środowisku odizolowanym od sieci (offline).

**XVI. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa – 2 szt. UPS;**

Minimalne wymagania dla jednej sztuki zasilacza UPS:

Moc	6 kVA
	6 kW

Klasyfikacja (PN-EN IEC 62040-3)		On-Line, podwójna konwersja, VFI SS111
Typ zabudowy		RACK
Wejście zasilanie -	Liczba faz	1
	Napięcie znamionowe	220 / 230 / 240 V
	Zakres napięcia	110 ÷ 275 V
	Częstotliwość znamionowa	50 / 60 Hz (autodetekcja)
	Zakres częstotliwości	40 ÷ 70 Hz
	Współczynnik mocy (PF)	≥ 0,995
	Zniekształcenia harmoniczne (THDi)	< 3 %
	Zgodność z systemem zasilania	TN
	Sposób podłączenia	P + N + PE (listwa zaciskowa)
Akumulatory	Technologia akumulatorów	VRLA / AGM
	Napięcie nominalne łańcucha akumulatorów	± 240 V DC
	Opcjonalne napięcie łańcucha akumulatorów	± 192 + 240 V DC
	Pojemność wewnętrznych akumulatorów	7 / 9 / 10 Ah
	Pojemność akumulatorów	dostosowana do wymaganej autonomii w zestawach EBM lub STB
	Prąd ładowania nominalny	12:00 AM
	Możliwość podłączenia zewnętrznych	zestawy EBM lub STB
Wyjście	Liczba faz	1
	Napięcie wyjściowe	220 / 230 / 240 V (konfigurowalne)
	Dokładność napięcia	± 1 %
	Częstotliwość dla pracy z sieci	synchronizowana
	Częstotliwość dla pracy z akumulatorów	50 / 60 Hz
	Przebieg napięcia	fala sinusoidalna
	Współczynnik mocy (PF)	1
	Współczynnik szczytu (CF)	3:1

	Zniekształcenia harmoniczne (THDu)	$\leq 1 \%$
	Zdolność przeciążeniowa	100 ÷ 105 % utrzymanie pracy
		105 ÷ 125 % przełączenie na bypass po 10 min
		125 ÷ 150 % przełączenie na bypass po 30 s > 150 % przełączenie na bypass po 500 ms
	Sposób podłączenia	P + N + PE (listwa zaciskowa) + 2 x IEC 60320 C13
System	Sprawność w trybie sieci	$\geq 95 \%$
	Sprawność w trybie ECO	$\geq 98 \%$
	Czas przełączenia	0 ms (ECO <-> inwerter: 10 ms)
	Interfejs użytkownika	obrotowy (90°) wyświetlacz punktowy LCD - j.polski
	Złącze EPO	tak
	Zabezpieczenia	zwarciovowe
		przeciążeniowe
		temperaturowe
	Filtr przeciwzakłóceńowy	RFI
		EMI
	Alarmy	przeciążenie
		praca z akumulatorów
		niskie napięcie akumulatorów
		awaria wentylatorów
	Praca w trybie konwersji	CVCF
	Praca równoległa	do 3 jednostek
	EMI	PN-EN IEC 62040-2 - kat. C3
	EMS	PN-EN 61000-4-2



Komunikacja	Interfejsy standardowe	PN-EN IEC 61000-4-3
		PN-EN 61000-4-4
		PN-EN 61000-4-5
		USB (typ B)
	Interfejsy opcjonalne	RS232
		Intelligent Slot
		styki bezpotencjałowe
		karty rozszerzeń:
	Obsługa systemów operacyjnych	WEB / SNMP
		RS485 / MODBUS
		styki bezpotencjałowe
		MS Windows / Linux / Unix / MacOS
Cechy	Wymiary (szer. x wys. x gł.)	438 x 86,2 x 573 mm
	Waga bez akumulatorów	13,6 kg
	Temperatura pracy	0 °C ÷ 40 °C
	Wilgotność	0 ÷ 95 % (bez kondensacji)
	Głośność (@ 1 m)	< 45 dB
	Stopień ochrony (PN-EN 60529:2003)	IP 20
	Montaż zasilacza	pionowy/RACK
	Wysokość robocza bez obniżenia mocy	0 ÷ 1000 m n.p.m.
	Wysokość robocza z obniżeniem mocy	obniżenie mocy o 1 % co 100 m
		w zakresie 1000 ÷ 3000 m n.p.m.

#### **XVII. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa – 1 szt.;**

Oferowany sprzęt musi być fabrycznie nowy i nieużywany przed dniem dostarczenia do siedziby Zamawiającego. Data produkcji nie może być wcześniejsza niż 2025 rok.

Minimalne wymagania techniczne:

- typ szafy: wolnostojąca
- pojemność stelaża: 42U
- szerokość: 800mm

- głębokość: 1000mm
- maksymalna waga przeznaczona do umieszczenia/przechowywania przez urządzenie: 1500 kg
- materiał wykonania: stal
- rodzaj ramy: zamknięty
- konstrukcja drzwi tylnych: stalowe perforowane umożliwiające przepływ powietrza
- konstrukcja drzwi przednich: stalowe perforowane umożliwiające przepływ powietrza
- zdejmowalne drzwi tylne: tak
- zdejmowalne drzwi przednie: tak
- zdejmowalne panele boczne: tak
- regulowane wymiary wejść kablowych na pokrywę górną i płytę dolną: tak
- możliwość otwierania drzwi na lewą lub prawą stronę: tak
- zamek: tak
- zamek klucza drzwi przednich: tak
- zamek na klucz panelu bocznego: tak
- relingi: tak
- regulowane nóżki (stopy): tak
- zgodność ze standardem montażu urządzeń 19"

#### **XVIII. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa;**

Przedmiotem zamówienia jest dostawa, instalacja, integracja, uruchomienie oraz wstępna konfiguracja infrastruktury informatycznej i bezpieczeństwa, obejmującej elementy sprzętowe, programowe i systemowe. Wdrożenie ma przygotować środowisko Zamawiającego do dalszej konfiguracji produkcyjnej oraz umożliwić bezpieczne i stabilne funkcjonowanie systemów.

Zakres obejmuje wdrożenie następujących komponentów:

Zakres wdrożeniowy

##### **1. Rozwiązanie typu XDR**

Wykonawca dostarcza oraz instaluje system zaawansowanego wykrywania i reagowania na zagrożenia, w tym:

- instalację agentów na wskazanych stacjach roboczych i serwerach,
- konfigurację połączenia z chmurą producenta,
- wdrożenie podstawowych polityk bezpieczeństwa,
- walidację komunikacji i logowania zdarzeń.

##### **2. Zapory sieciowe nowej generacji (NGFW)**

Wykonawca dokonuje wdrożenia zapór brzegowych, obejmującego:

- instalację w szafie RACK,

- włączenie i podstawową konfigurację trybu pracy (routed/transparent),
- konfigurację podstawowych reguł ruchu,
- włączenie inspekcji SSL/TLS,
- integrację zapory z systemem SIEM, XDR i systemem zarządzania.

### 3. Serwery fizyczne

Wykonawca dostarcza i uruchamia serwery zgodnie z projektowaną architekturą, w tym:

- montaż w szafie RACK,
- konfigurację macierzy RAID,
- aktualizację firmware (BIOS, BMC, kontrolery RAID/NVMe, NIC),
- przygotowanie serwerów pod system wirtualizacji lub systemy fizyczne.

### 4. Przełączniki zarządzalne

Zakres obejmuje:

- montaż switchy, podłączenie do sieci,
- konfigurację podstawową (adresacja, VLAN, trunk/access),
- konfigurację protokołów zarządzania (SSH, SNMPv3, syslog),
- testy ciągłości i przepustowości łącza.

### 5. Punkty dostępowe Wi-Fi

Wykonawca:

- instaluje access pointy w miejscach wskazanych i przygotowanych przez Zamawiającego,
- paruje je z kontrolerem sieciowym,
- uruchamia podstawowe SSID oraz szyfrowanie WPA2/WPA3,
- weryfikuje zasięg i stabilność transmisji.

### 6. Oprogramowanie NAC

Wdrożenie obejmuje:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatknie VLAN-u gościnnego, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.

### 7. System operacyjny serwerowy + licencje CAL

Zakres:

- instalacja systemu operacyjnego na serwerach,
- konfiguracja usług podstawowych (rola AD, DNS, DHCP),
- aktywacja licencji CAL.

#### 8. System IDS dedykowany sieci OT

Wykonawca:

- instaluje sondy IDS w segmentach OT,
- uruchamia serwer główny analityki,
- integruje czujniki z SIEM,
- testuje odbiór logów i alarmów.

#### 9. System SIEM

Wykonawca wykonuje:

- Przeprowadzenie instalacji i konfiguracji systemu SIEM/SOAR.
- Podłączenie do systemu wskazanych przez Zamawiającego w OPZ źródeł danych.
- Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.
- Jeżeli oferowany system SIEM nie posiada predefiniowanych parserów, wizualizacji, dashboardów oraz reguł korelacyjnych Wykonawca jest zobligowany do ich implementacji na etapie wdrożenia.

#### 10. Dwa urządzenia NAS

Zakres:

- montaż w RACK,
- konfiguracja RAID,
- utworzenie udziałów plikowych,
- integracja z AD,
- włączenie snapshotów.

#### 11. System wirtualizacji

Wykonawca:

- instaluje hypervisor bezpośrednio na serwerach,
- tworzy klaster, vSwitch, datastore,
- wykonuje testy HA i vMotion (lub równoważnych mechanizmów).

#### 12. Appliance do backupu

Zakres wdrożenia obejmuje:

- instalację urządzenia,
- konfigurację repozytoriów,
- utworzenie zadań backupu dla serwerów, NAS i stacji roboczych.

### 13. Usługa kopii zapasowych w chmurze

Wykonawca uruchamia mechanizm backupu hybrydowego poprzez:

- konfigurację kanału komunikacyjnego z chmurą,
- utworzenie harmonogramów wysyłki,
- test backupu i odtworzenia.

### 14. Oprogramowanie monitorujące

Wdrożenie obejmuje:

- instalację serwera monitoringu,
- automatyczne wykrywanie urządzeń,
- konfigurację alertów i powiadomień.

### 15. System open source do informatyki śledczej

Wykonawca:

- instaluje narzędzie na wskazanych stacjach,
- konfiguruje moduły analizy obrazów dysków, artefaktów systemowych, logów,
- testuje obsługę formatów E01, RAW, AFF.

### 16. UPS-y

Wykonawca wykonuje:

- montaż UPS-ów,
- podłączenie do obwodów zasilania,
- kalibrację,
- integrację z serwerami (shutdown management).

### 17. Szafa RACK

Wykonawca:

- dostarcza i montuje szafę,
- organizuje okablowanie,
- instaluje urządzenia z zachowaniem zasad przepływu powietrza.

### 3. Testy wdrożeniowe

Wykonawca przeprowadza testy:

- łączności i przepustowości,
- działania systemów backupowych,
- rejestracji zdarzeń w SIEM,
- działania polityk NAC,
- poprawnego działania klastrów wirtualizacji.



## **XIX. Usługa konfiguracji i hardeningu systemów/urządzeń;**

Przedmiotem zamówienia jest wykonanie zaawansowanej konfiguracji, optymalizacji, hardeningu oraz zabezpieczenia wszystkich modułów sprzętowych i programowych dostarczonych w ramach projektu, w oparciu o uznane standardy bezpieczeństwa.

Zakres zaawansowanej konfiguracji i hardeningu

1. Hardening urządzeń sieciowych (NGFW, przełączników, AP)
  - 1) Konfiguracja zaawansowanych reguł ruchu, filtracji, inspekcji warstw aplikacyjnych.
  - 2) Wdrożenie mechanizmów IDS/IPS.
  - 3) Konfiguracja rozdzielania ruchu sieciowego (segmentacja, VLAN, ACL).
  - 4) Włączenie protokołów szyfrowanych (TLS, SSH, SNMPv3).
  - 5) Implementacja polityk bezpieczeństwa zgodnych z CIS lub NIST.
  - 6) Blokowanie nieużywanych portów, usług, protokołów.
2. Hardening systemów serwerowych
  - 1) Konfiguracja polityk bezpieczeństwa systemu operacyjnego.
  - 2) Włączenie szyfrowania dysków.
  - 3) Audytacja uprawnień użytkowników i grup.
  - 4) Instalacja i konfiguracja agentów SIEM, XDR, monitoringu.
3. Hardening platformy wirtualizacyjnej
  - 1) Konfiguracja zabezpieczeń hypervisorów.
  - 2) Polityki izolacji ruchu zarządzającego.
  - 3) Ustawienia HA, DRS, zabezpieczenia VM-ów.
  - 4) Hardening dostępu administracyjnego.
4. Zaawansowana konfiguracja SIEM
  - 1) Opracowanie reguł korelacyjnych zgodnych z profilem organizacji.
  - 2) Integracja z XDR, NGFW, IDS, serwerami, NAS, wirtualizacją.
  - 3) Opracowanie dashboardów i alertów wysokiego priorytetu.
  - 4) Konfiguracja retencji logów zgodnie z polityką.
5. Zaawansowana konfiguracja XDR
  - 1) Definicja polityk ochrony punktów końcowych.
  - 2) Konfiguracja mechanizmów automatycznej reakcji (SOAR).
  - 3) Integracja z systemem SIEM.
6. Konfiguracja NAC
  - 1) Polityki autoryzacji 802.1X dla użytkowników i urządzeń.

- 2) Profilowanie urządzeń IoT/OT.
- 3) Mechanizmy dynamicznego VLAN.

#### 7. Hardening NAS i backupu

- 1) Ograniczenie dostępu do udziałów, SMB hardening.
- 2) Konfiguracja retencji i snapshotów.
- 3) Implementacja georedundancji (backup do chmury).
- 4) Test odtwarzania danych.

#### 8. Hardening UPS i infrastruktury fizycznej

- 1) Konfiguracja sieci zarządzania UPS.
- 2) Integracja z monitoringiem.
- 3) Testy przełączania zasilania.

#### 9. Hardening i konfiguracja systemu forensic open source

1. Konfiguracja modułów do analizy artefaktów.
2. Utwardzenie systemu pracującego offline.
3. Testy analiz obrazów dyskowych i logów.

