OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa dla Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Radzyminie

1. Informacje ogólne

1.1. Nazwa zamówienia

Nazwa zamówienia:" Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa dla Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Radzyminie"
Przedmiotem zamówienia jest dostawa, wdrożenie, konfiguracja, integracja, hardening, uruchomienie, przetestowanie, udokumentowanie oraz wsparcie powdrożeniowe zintegrowanego rozwiązania cyberbezpieczeństwa IT/OT dla Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Radzyminie, realizowanego w ramach Projektu „Zwiększenie cyberbezpieczeństwa Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Radzyminie" dofinasowanego ze środków Instrumentu na rzecz Odbudowy i Zwiększenia Odporności oraz Unii Europejskie j- NextGeneration EU, projektu grantowego „Cyberbezpieczne Wodociągi" .

1.2. Cel zamówienia

Celem zamówienia jest podniesienie poziomu cyberbezpieczeństwa środowiska IT/OT Zamawiającego poprzez dostarczenie i wdrożenie spójnego rozwiązania.

1.3. Charakter zamówienia

Zamówienie stanowi jeden zintegrowany pakiet technologiczny. Obejmuje zarówno dostawę sprzętu, oprogramowania i licencji, jak również czynności niezbędne do uruchomienia, skonfigurowania, zintegrowania, zabezpieczenia, przetestowania i odbioru rozwiązania.
Zamawiający nie dopuszcza realizacji przedmiotu zamówienia jako zbioru niezależnych dostaw bez zapewnienia odpowiedzialności Wykonawcy za wdrożenie, integrację i działanie całości rozwiązania.

2. Zakres zamówienia

2.1. Zakres podstawowy

Przedmiot zamówienia obejmuje dostawę i wdrożenie następujących komponentów:

1. oprogramowania typu XDR dla stacji roboczych i serwerów — 25 urządzeń końcowych objętych ochroną,
2. urządzeń UTM/firewall dla lokalizacji objętych projektem 5 szt.,
3. serwerów fizycznych niezbędnych do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA — 3 szt.,
4. zarządzalnych urządzeń sieciowych z obsługą VLAN, MACsec, standardu 802.1x (switch) – 2 szt. switch typ I, 2 szt. switch typ II;
5. oprogramowania/licencji NAC dla 150 urządzeń końcowych,
6. systemu operacyjnego serwerowego, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa - 3 szt.,
7. licencji dostępowych CAL, do systemu, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – licencje dla 25 użytkowników;
8. oprogramowania SIEM, wdrożenie system typu opensource,
9. urządzeń NAS — 2 szt.,
10. środowiska wirtualizacyjnego, dedykowanego do systemów, na których zostanie zainstalowany produkt z zakresu cyberbezpieczeństwa,
11. serwera do wykonywania kopii zapasowych – 1 szt. serwera do backupu
12. oprogramowania do monitorowania infrastruktury informatycznej, wdrożenie system typu opensource,
13. narzędzia do analizy powłamaniowej i zabezpieczania dowodów cyfrowych, wdrożenie systemu typu opensource,
14. systemu MFA,

15. szafy RACK, do produktów i rozwiązań z zakresu bezpieczeństwa – 1 szt.,
16. oprogramowania do zarządzania podatnościami,
17. usług wdrożenia, konfiguracji, integracji, hardeningu, testów i odbiorów,
18. usług utrzymania i wsparcia powdrożeniowego,
19. szkolenia specjalistycznego administratorów i osób odpowiedzialnych za eksploatację wdrożonych rozwiązań.

2.2. Zakres usług Wykonawcy

W ramach realizacji zamówienia Wykonawca zobowiązany jest w szczególności do:

1. przeprowadzenia analizy przedwdrożeniowej w zakresie niezbędnym do prawidłowej realizacji zamówienia,
2. opracowania i uzgodnienia z Zamawiającym planu realizacji,
3. dostawy sprzętu, oprogramowania i licencji,
4. instalacji urządzeń i oprogramowania,
5. konfiguracji podstawowej i zaawansowanej,
6. integracji komponentów rozwiązania,
7. wykonania hardeningu dostarczonych i wdrażanych komponentów,
8. wykonania testów funkcjonalnych, konfiguracyjnych, integracyjnych i odbiorowych,
9. sporządzenia dokumentacji powdrożeniowej,
10. przeprowadzenia szkolenia specjalistycznego dla administratorów,
11. zapewnienia wsparcia powdrożeniowego i utrzymaniowego w zakresie określonym w OPZ i umowie,
12. udziału w procedurze odbiorów cząstkowych i odbioru końcowego.

2.3. Wyłączenia z zakresu zamówienia

Przedmiot niniejszego zamówienia nie obejmuje świadczenia usługi SOC; niniejsze zamówienie obejmuje jedynie techniczne przygotowanie środowiska do późniejszej integracji z usługą SOC. Wymagania dotyczące SIEM należy rozumieć jako wymagania techniczne wobec dostarczanego rozwiązania, a nie jako obowiązek świadczenia usługi SOC.

3. Środowisko objęte wdrożeniem

3.1. Lokalizacje

Rozwiązanie obejmuje środowisko Zamawiającego w następujących lokalizacjach:

1. Siedziba PWiK, ul. Komunalna 2 w Radzyminie
2. Oczyszczalnia Ścieków Komunalnych (OŚK), ul. Księżycowa 13 w Radzyminie
3. Stacja Uzdatniania Wody (SUW), ul. Batalionów Chłopskich 8 w Radzyminie

3.2. Charakter środowiska

Środowisko Zamawiającego obejmuje elementy IT oraz wybrane elementy OT istotne z punktu widzenia cyberbezpieczeństwa, w szczególności styków IT/OT, komunikacji sieciowej, dostępu zdalnego, monitoringu, backupu, kontroli dostępu i segmentacji.
Wykonawca jest zobowiązany prowadzić prace w sposób minimalizujący ryzyko zakłócenia ciągłości działania Zamawiającego, w szczególności w odniesieniu do systemów i lokalizacji wspierających działalność operacyjną przedsiębiorstwa wodociągowo-kanalizacyjnego.

4. Wymagania ogólne dla rozwiązania

4.1. Wymagania architektoniczne

Rozwiązanie powinno obejmować lub wspierać:

1. spójny system cyberbezpieczeństwa IT/OT,
2. centralne zarządzanie kluczowymi mechanizmami bezpieczeństwa,
3. segmentację sieci i separację ruchu IT/OT,
4. centralizację logów i zdarzeń bezpieczeństwa,
5. monitoring dostępności i stanu infrastruktury,

6. ochronę sieci i styku z Internetem,
7. ochronę stacji roboczych i serwerów,
8. centralizację logów i zdarzeń bezpieczeństwa,
9. backup i odtwarzanie danych,
10. ochronę dostępu uprzywilejowanego,
11. analizy incydentów i działań powłamaniowych,
12. zarządzanie podatnościami,
13. współpracę z usługą SOC nabywaną w odrębnym postępowaniu,
14. możliwość dalszej eksploatacji przez administratorów Zamawiającego.

4.2. Wymagania dotyczące neutralności technologicznej

1. Wszelkie wskazania nazw własnych, technologii, producentów, znaków towarowych lub konkretnych funkcjonalności charakterystycznych dla danego producenta należy rozumieć jako wskazania przykładowe, dopuszczające rozwiązania równoważne, o ile spełniają one wymagania funkcjonalne, wydajnościowe, bezpieczeństwa, integracyjne i eksploatacyjne określone w OPZ.
2. Wykonawca oferujący rozwiązanie równoważne jest zobowiązany wykazać równoważność poprzez przedstawienie odpowiednich dokumentów, opisów technicznych, kart katalogowych, oświadczeń producenta lub innych środków dowodowych potwierdzających spełnienie wymagań OPZ.

4.3. Wymagania dotyczące bezpieczeństwa

Rozwiązanie powinno być wdrożone zgodnie z dobrymi praktykami bezpieczeństwa, w szczególności z uwzględnieniem:

1. zasady minimalnych uprawnień,
2. rozdzielenia ról administracyjnych,
3. wyłączenia nieużywanych usług, portów i protokołów,
4. aktualizacji firmware, systemów i oprogramowania,
5. bezpiecznej konfiguracji kont administracyjnych,
6. logowania zdarzeń istotnych z punktu widzenia cyberbezpieczeństwa,
7. dokumentowania wykonanych zmian konfiguracyjnych.

Zasady bezpieczeństwa pracy Wykonawcy opisane są w Rozdz. 8.

4.4 Hardening

1. Wykonawca zobowiązany jest wykonać hardening wszystkich dostarczonych i wdrażanych komponentów w zakresie niezbędnym do ich bezpiecznego uruchomienia, integracji, administracji i utrzymania.
2. Hardening musi obejmować co najmniej:
    1. konfigurację kont administracyjnych zgodnie z zasadą minimalnych uprawnień,
    2. rozdzielenie ról administracyjnych, jeżeli wspiera to dane rozwiązanie,
    3. zastosowanie uwierzytelniania wieloskładnikowego tam, gdzie jest to wymagane w OPZ albo technicznie dostępne i uzasadnione,
    4. ograniczenie dostępu administracyjnego do niezbędnych adresów, kont, ról i kanałów komunikacji,
    5. wykorzystywanie szyfrowanych kanałów administracyjnych,
    6. wyłączenie albo ograniczenie nieużywanych usług, portów, protokołów i kont,
    7. aktualizację firmware, systemów operacyjnych i oprogramowania do wersji uzgodnionych z Zamawiającym,
    8. konfigurację logowania zdarzeń istotnych z punktu widzenia cyberbezpieczeństwa,
    9. przekazywanie logów do systemu SIEM albo innego właściwego komponentu, jeżeli jest to przewidziane w OPZ,
    10. konfigurację podstawowych polityk bezpieczeństwa dla wdrażanych systemów,
    11. zabezpieczenie konfiguracji komponentów przed nieuprawnioną zmianą,
    12. wykonanie kopii konfiguracji komponentów, jeżeli dane rozwiązanie to umożliwia,
    13. ograniczenie i rejestrowanie dostępu Wykonawcy do środowiska Zamawiającego,

14. udokumentowanie wykonanych ustawień bezpieczeństwa i zmian konfiguracyjnych.

Wykonawca zobowiązany jest uwzględnić hardening w dokumentacji powdrożeniowej, w szczególności poprzez opisanie wykonanych ustawień bezpieczeństwa, zastosowanych kont i ról administracyjnych, mechanizmów dostępu, logowania, aktualizacji oraz kopii konfiguracji.

4.5 Utrzymanie i eksploatacja

1. Przedmiot usługi
W ramach realizacji zamówienia Wykonawca będzie świadczył usługę utrzymania i eksploatacji wdrożonego środowiska obejmującego dostarczone urządzenia, oprogramowanie oraz rozwiązania z zakresu cyberbezpieczeństwa, w szczególności:

- rozwiązanie klasy XDR,
- system UTM,
- serwery fizyczne,
- zarządzalne przełączniki sieciowe,
- system NAC,
- system SIEM,
- serwer NAS,
- środowisko wirtualizacyjne,
- serwer do wykonywania kopii zapasowych,
- oprogramowanie do monitorowania infrastruktury informatycznej,
- narzędzie do analizy powłamaniowej,
- oprogramowanie do zarządzania podatnościami,
- pozostałe elementy dostarczone w ramach realizacji zamówienia.

Usługa ma charakter wsparcia powdrożeniowego i obejmuje pomoc techniczną oraz ekspercką w zakresie eksploatacji wdrożonego środowiska. Usługa nie obejmuje przejęcia przez Wykonawcę obowiązków związanych z bieżącym administrowaniem infrastrukturą Zamawiającego.

2. Zakres usługi
W ramach usługi Wykonawca zobowiązany jest do:

1. Świadczenia konsultacji technicznych dotyczących eksploatacji wdrożonych rozwiązań.
2. Wsparcia Zamawiającego w diagnozowaniu i usuwaniu problemów związanych z funkcjonowaniem dostarczonych urządzeń i oprogramowania.
3. Wprowadzania zmian konfiguracyjnych wynikających z bieżących potrzeb Zamawiającego, w szczególności:
    - modyfikacji polityk bezpieczeństwa,
    - zmian konfiguracji urządzeń sieciowych,
    - zmian konfiguracji systemów bezpieczeństwa,
    - dostosowania konfiguracji do zmian w infrastrukturze Zamawiającego,
    - aktualizacji reguł, polityk, profili oraz parametrów pracy systemów.
4. Wsparcia przy analizie zdarzeń związanych z funkcjonowaniem wdrożonych rozwiązań oraz wskazywania sposobu ich usunięcia.
5. Udzielania pomocy przy odtwarzaniu poprawnej pracy środowiska po awariach dotyczących dostarczonych rozwiązań.
6. Wsparcia przy analizie wyników monitorowania infrastruktury, analizy podatności oraz działania systemów bezpieczeństwa.
7. Współpracy z producentami dostarczonych rozwiązań w przypadku konieczności eskalacji zgłoszeń serwisowych.
8. Udzielania wyjaśnień dotyczących działania wdrożonych rozwiązań oraz rekomendowania dobrych praktyk eksploatacyjnych.

3. Sposób świadczenia usługi

1. Usługa będzie świadczona zdalnie, z możliwością realizacji wsparcia w siedzibie Zamawiającego, jeżeli Wykonawca uzna, że charakter zgłoszenia będzie tego wymagał.

2. Zgłoszenia będą przyjmowane za pośrednictwem poczty elektronicznej, systemu zgłoszeniowego Wykonawcy lub telefonicznie.
3. Wykonawca zapewni obsługę zgłoszeń przez personel posiadający kwalifikacje i doświadczenie adekwatne do wdrożonych rozwiązań.
4. Dostępność: Pon.-Pt., w godz. 8:00 – 16:00 lub po ustaleniu z Wykonawcą w innych godzinach.
5. W zakresie planowanych prac Zamawiający ustali drogą mailową lub telefoniczną przedmiot oraz termin prac z co najmniej 3-dniowym wyprzedzeniem.
6. Wszystkie wykonane zmiany konfiguracyjne powinny zostać udokumentowane i przekazane Zamawiającemu.

4. Ograniczenia zakresu usługi
Usługa nie obejmuje:
1. bieżącego administrowania środowiskiem informatycznym Zamawiającego;
2. stałego monitorowania infrastruktury przez Wykonawcę;
3. wykonywania codziennych czynności administracyjnych;
4. zarządzania użytkownikami systemów informatycznych Zamawiającego;
5. rozwoju infrastruktury poprzez wdrażanie nowych funkcjonalności wykraczających poza zakres zamówienia;
6. świadczenia usług typu SOC, NOC lub outsourcingu IT.

5. Rezultat świadczenia usługi
Celem usługi jest zapewnienie Zamawiającemu dostępu do specjalistycznego wsparcia technicznego umożliwiającego utrzymanie prawidłowej pracy wdrożonych rozwiązań, sprawne usuwanie problemów eksploatacyjnych, bezpieczne wprowadzanie zmian konfiguracyjnych oraz utrzymanie wymaganej funkcjonalności środowiska w całym okresie obowiązywania umowy.

5. Wymagania wspólne dla komponentów rozwiązania

1. Wszystkie komponenty sprzętowe dostarczane w ramach zamówienia muszą być fabrycznie nowe, nieużywane, wolne od wad fizycznych i prawnych, pochodzić z oficjalnego kanału dystrybucji producenta lub autoryzowanego dystrybutora oraz być dopuszczone do użytkowania na rynku Unii Europejskiej.
2. Wszystkie dostarczane licencje, subskrypcje, tokeny, prawa do aktualizacji oraz prawa do wsparcia muszą być legalne, prawidłowo przypisane do Zamawiającego i umożliwiać korzystanie z dostarczonych komponentów zgodnie z celem zamówienia.
3. Wykonawca musi dostarczyć rozwiązanie kompletne, tj. obejmujące wszystkie elementy sprzętowe, programowe, licencyjne, konfiguracyjne i integracyjne niezbędne do uruchomienia i odbioru rozwiązania zgodnie z OPZ.
4. Wykonawca odpowiada za kompatybilność dostarczanych komponentów oraz za ich integrację w jeden spójny system cyberbezpieczeństwa IT/OT.
5. Wykonawca musi zapewnić, że dostarczone komponenty będą mogły być administrowane, aktualizowane, monitorowane i utrzymywane przez Zamawiającego po zakończeniu wdrożenia.
6. Wykonawca musi dostarczyć dokumentację producenta lub równoważne dokumenty techniczne potwierdzające spełnienie wymagań OPZ przez oferowane komponenty.
7. Wymagania wskazane w niniejszym rozdziale mają charakter minimalny. Wykonawca może zaoferować rozwiązania o parametrach lepszych, pod warunkiem zachowania zgodności z OPZ, wymaganiami integracyjnymi oraz zasadami bezpieczeństwa.
8. Wszystkie komponenty muszą zostać objęte dokumentacją powdrożeniową, testami odbiorowymi oraz wymaganiami dotyczącymi gwarancji, aktualizacji, wsparcia i utrzymania określonymi w OPZ i umowie.

6. Zasada wdrożenia zintegrowanego rozwiązania

1. Przedmiot zamówienia obejmuje nie tylko dostawę sprzętu, oprogramowania, licencji i subskrypcji, lecz także ich uruchomienie, konfigurację, integrację, hardening, przetestowanie i przekazanie do eksploatacji jako jednego spójnego rozwiązania cyberbezpieczeństwa IT/OT.

2. Wykonawca odpowiada za kompletność, kompatybilność i współdziałanie wszystkich dostarczonych oraz wdrażanych komponentów w zakresie niezbędnym do osiągnięcia celu zamówienia i spełnienia wymagań OPZ.
3. W przypadku rozbieżności pomiędzy ogólnym opisem rozwiązania a wymaganiami szczegółowymi dla danego komponentu, pierwszeństwo mają wymagania szczegółowe określone w rozdziale 7 OPZ, o ile nie są sprzeczne z wymaganiami umowy i dokumentów zamówienia.

7. Wymagania szczegółowe dla komponentów rozwiązania

7.1 Oprogramowanie typu XDR (Extended Detection and Response)

Wymagania ogólne

1. Ochrona 25 stacji - licencja oprogramowania XDR.
2. Okres do 31 grudnia 2026 r.

Wymagane funkcjonalności:

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu http Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
10. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
11. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
15. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
16. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
17. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
18. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
19. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
20. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
21. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
22. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 100 kategorii i podkategorii.
23. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
24. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowsze oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, UbuntuServer 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
9. Dodatkowe wymagania dla ochrony serwerów Windows:

a. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
b. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
c. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
d. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
e. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
f. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
g. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
h. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
i. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

10. Dodatkowe wymagania dla ochrony serwerów Linux:
    a. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    b. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
    c. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS .
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    a. usunięcie zawartości urządzenia,
    b. przywrócenie urządzenie do ustawień fabrycznych,
    c. zablokowania urządzenia,
    d. uruchomienie sygnału dźwiękowego,
    e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
    a. nazwę aplikacji,
    b. nazwę pakietu,
    c. kategorię sklepu Google Play,
    d. uprawnienia aplikacji,
    e. epochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. Czysty,
    b. Podejrzany,
    c. Bardzo podejrzany,
    d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
9. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

10. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
11. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
12. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
13. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
14. Konsola administracyjna musi mieć możliwość tagowania obiektów.
15. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

7.2. UTM

Wymagania Ogólne

1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.
2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
4. System wspiera protokoły IPv4 oraz IPv6 w zakresie:
    - Firewall.
    - Ochrony w warstwie aplikacji.
    - Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
5. System ma pracować w postaci redundantnego klastra.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
    - 10 portami Gigabit Ethernet RJ-45.
    - Urządzenie musi być przystosowane do montażu w szafie RACK 19" i posiadać dostęp do portów RJ-45 od przodu urządzenia.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tyś. jednoczesnych połączeń oraz 34 tyś. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6.3 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 0.7 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 0.6 Gbps.

Funkcje Systemu Bezpieczeństwa:
W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure.
    - Cisco ACI.
    - Google Cloud Platform (GCP).

- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19, 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
    - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
    - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
    - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
    - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
    - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.

4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
2. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
3. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
4. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
5. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
6. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
7. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
8. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    - Haseł dynamicznych w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i

raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje
Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do 31 grudnia 2026r.

Gwarancja oraz wsparcie
Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub dystrybutora lub wykonawcę przez okres wymaganej gwarancji.

7.3. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA

Wymagania ogólne

- serwer fizyczny – 3 szt.

Minimalne wymagania dla jednego serwera:

Nazwa elementu, parametru lub cechy	**Opis wymagań Serwerów**
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
Procesor	• 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 (www.spec.org), dla serwera oferowanego producenta.
Liczba zainstalowanych procesorów	2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje

Pamięć operacyjna	• Zainstalowane minimum 128GB pamięci RAM o częstotliwości 6400MHz. • Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Rozbudowa dysków	• 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. • Wymagany jest wewnętrzny slot na kartę Micro SD.
Zasilacz	• Minimum dwa redundantne zasilacze o mocy minimum 800W z certyfikatem minimum Titanium. • Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowane dwuportowa karta 10GBASE-T. Karta nie może zajmować żadnego ze slotów PCIe. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Sloty I/O	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 x8 z czego jeden High-Profile, oraz jeden slot PCIe wewnątrz obudowy serwera dedykowany pod kontroler dyskowy.
Dodatkowe porty	• z przodu obudowy: możliwość instalacji 2x USB 3 (z czego jeden z możliwością zarządzania serwerem) , zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu Mini DisplayPort • z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: Możliwość instalacji portu USB 3 wewnątrz obudowy. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port na kartę Micro SD powinny być umieszczone jako element konstrukcyjny serwera zapewniający wymaganą funkcjonalność, dostępność interfejsów oraz możliwość serwisowania.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony jako element konstrukcyjny serwera zapewniający wymaganą funkcjonalność, dostępność interfejsów oraz możliwość serwisowania. 1. Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna 2. Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja 3. Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. 4. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. 5. Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 6. Update systemowego firmware 7. Monitoring i możliwość ograniczenia poboru prądu 8. Zdalne włączanie/wyłączanie/restart 9. Zapis video zdalnych sesji 10. Podmontowanie lokalnych mediow z wykorzystaniem Java client 11. Przekierowanie kosnoli szeregowej przez IPMI

	12. Zrzut ekranu w momencie zawieszenia systemu 13. Możliwość przejęcia zdalnego ekranu 14. Możliwość zdalnej instalacji systemu operacyjnego 15. Alerty Syslog 16. Przekierowanie konsoli szeregowej przez SSH 17. Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera 18. Możliwość mapowania obrazów ISO z lokalnego dysku operatora 19. Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS 20. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę 21. wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API 22. Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. 23. Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję typu RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. 24. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. 25. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. 26. Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: 1. zarzadzanie infrastruktura serwerówi storage bez udziału dedykowanego agenta 2. przedstawianie graficznej reprezentacji zarządzanych urządzeń 3. możliwość skalowania do minimum 1000 urządzeń 4. obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 5. wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych 6. udostępnianie szybkiego podgląd stanu środowiska udostępnianie podsumowania stanu dla każdego urządzenia tworzenie alertów przy zmianie stanu urządzenia 7. monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, 8. konsola zarzadzania oparta o HTML 5 9. 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, 10. automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja 11. możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania 12. definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań 13. definiowanie roli użytkowników oprogramowania 14. obsługa REST API oraz Windows PowerShell

	15. obsługa SNMP, SYSLOG, Email Forwarding 16. autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML 17. obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami 18. przedstawianie historycznych aktywności użytkowników 19. blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych 20. tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv 21. Obsługa NTP 22. przesyłanie alertów do konsoli firm trzecich 23. tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) 24. instalowanie systemów operacyjnych oraz wirtalizatorów 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 przesylem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, Splunk.
Funkcje zabezpieczeń	• Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony jako element konstrukcyjny serwera zapewniający wymaganą funkcjonalność, dostępność interfejsów oraz możliwość serwisowania) 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.
Obsługa	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.
Diagnostyka	• 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 awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
Systemy operacyjne	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

Gwarancja	• 36 miesiący gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. • Uszkodzone nośniki danych pozostają własnością zamawiącego. • 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..

7.4 Zarządzalne urządzenia sieciowe

Wymagania ogólne

- obsługa VLAN, MACsec, standard 802.1x (switch)
- switch typ I - 2 szt.
- switch typ II - 2 szt.

Minimalne wymaganie dotyczące jednej sztuki przełącznika dostępowego:

7.4.1.Switch typ I:

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:
    1. możliwość montażu w stelażu/szafie 19”
    2. wysokość maksymalna 1U
    3. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
    4. minimum jeden zasilacz 230V AC
    5. zakres temperatur pracy ciągłej co najmniej od 0°C do +40 °C
    6. zakres wilgotności pracy co najmniej 10% - 90%
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
    1. 48 portów 100/1000BASE-T zgodne ze standardem 802.3at (minimalny budżet mocy PoE: 370W)
    2. porty 10GE SFP+
    3. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4. Przełącznik musi posiadać następujące porty służące do zarządzania:
    1. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
5. Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 130 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 120 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:
    1. IGMP Snooping v2 i v3
    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:
    1. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu
    2. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    3. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
    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.

7.4.2. Switch typ II – 2 szt.

Wymagania ogólne

1. Typ urządzenia: Zarządzalny przełącznik warstwy 3 (L3), montowany w szafie rack 19"
2. Waga: max. 5 kg
3. Chłodzenie: Przepływ powietrza z przodu do tyłu, 4 wentylatory
4. Zasilanie: Wewnętrzny zasilacz AC 100–240 V (50/60 Hz), możliwość instalacji drugiego zasilacza (redundancja)
5. Pobór mocy: max. 89 W
6. Certyfikaty: FCC, RoHS
7. Gwarancja: 3 lata

Porty i interfejsy

1. Porty SFP+ (10G): 26 x 1/10GBase-X
2. Porty SFP28 (25G): 6 x 10/25GBase-X
3. Porty zarządzające:
    - 1 x RJ-45 (Console)
    - 1 x RJ-45 (Management)
    - 2 x USB 3.0 Type-A
    - 1 x USB-C (Console)
4. Maksymalna liczba urządzeń w stosie: min. 8

Wydajność i pojemność

1. Przepustowość przełączania: min. 820 Gbps
2. Przepustowość przekazywania: min. 410 Gbps
3. Przepustowość stosu: min. 300 Gbps
4. Szybkość przekazywania pakietów: min. 605 Mpps
5. Bufor pakietów: 8 MB

6. Tabela adresów MAC: min. 128 000 wpisów
7. Obsługa ramek jumbo: do 9 KB

Funkcje warstwy 3

1. Protokoły routingu:
    - Statyczne routowanie IPv4/IPv6
    - RIP v1/v2/v3
    - OSPF v2/v3
    - VRRP v2/v3
    - ECMP (do 256 wpisów)
    - RIPng
    - PIM-DM (Multicast)
    - MLDv2 (Multicast)
2. Tablica tras IPv4: do 102 400
3. Tablica tras IPv6: do 51 200
4. Grupy VRRP: do 64
5. Grupy IGMP: do 4 093
6. Grupy VLAN: do 4 000
7. Grupy LAG (Link Aggregation): do 120
8. Grupy ERPS (Ethernet Ring Protection Switching): do 64
9. Grupy QinQ (VLAN VPN): do 256

Funkcje bezpieczeństwa

1. ACL (Access Control Lists)Wsparcie dla IPv4 i IPv6
2. Dynamic ARP Inspection (DAI): Ochrona przed spoofingiem ARP
3. IEEE 802.1X: Uwierzytelnianie portów
4. MAB (MAC Authentication Bypass): Uwierzytelnianie na podstawie adresu MAC
5. Port Security: Ograniczenie dostępu do portów na podstawie adresów MAC
6. SSH v2: Zdalne zarządzanie z szyfrowaniem
7. RADIUS/TACACS+: Zewnętrzne serwery uwierzytelniające
8. BPDU Protection: Ochrona przed atakami BPDU
9. IP Source Guard: Ochrona przed spoofingiem źródła IP
10. DHCP Snooping: Monitorowanie i kontrola serwerów DHCP
11. Dynamic Host Configuration Protocol (DHCP) Relay: Przekazywanie żądań DHCP między
12. serwerami
13. MLD Snooping: Monitorowanie grup multicastowych IPv6
14. DHCPv6 Snooping: Monitorowanie i kontrola serwerów DHCPv6
15. ARP Inspection: Weryfikacja poprawności komunikatów ARP
16. Port Isolation: Izolacja portów w ramach VLAN
17. Guest VLAN: Tworzenie oddzielnych VLAN dla gości
18. Private VLAN: Izolacja portów w ramach tego samego VLAN
19. Voice VLAN: Priorytetyzacja ruchu VoIP

7.5. Oprogramowanie / licencje NAC (Network Access Control)

Wymagania ogólne

- 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 50 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 dostępu 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, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, 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 obsługę 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 rejestracje 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 konfiguracje 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 urządzeniu, 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, minumum 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 (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    - Microsoft Windows
    - Mac OS

- iOS
- Android

63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory 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:
    1. Tożsamość/Urządzenie końcowe,
    2. Grupa tożsamości/urządzeń końcowych,
    3. Parametry urządzeń końcowych, min: system operacyjny, wersja,
    4. Atrybuty Active Directory,
    5. Jednostka organizacyjna tożsamości/urządzeń końcowych,
    6. Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
    7. Grupy urządzeń sieciowych,
    8. Porty urządzeń sieciowych,
    9. Grupy portów urządzeń sieciowych,
    10. Jednostka organizacyjna portów,
    11. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
    12. Data, czas ważności polityki,
    13. Wewnętrzny Captive Portal,
    14. 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

21. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
22. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    1. możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    2. możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    3. Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
    4. 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:
    1. Uruchamianie usługi dla wybranych podsieci,
    2. Przypisanie ustalonego adresu IP dla adresu MAC.
    1. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
    2. Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
    3. Możliwość określania braku dostępu dla wybranych adresów MAC,
    4. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
    5. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
    6. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
    7. Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
    8. Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów 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 nadam 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 wpierać 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.
3. Alarmy mogą być generowane w sytuacjach, min:

- Ilości obsługiwanych transakcji RADIUS,
- Opóźnienie obsługi transkacji 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 31.12.2026 r. Licencja ta powinna obejmować minimum:

1. Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
2. Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
3. Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
4. Dostęp do dokumentacji i instrukcji na stronie internetowej.
5. Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

7.6. System operacyjny

Wymagania ogólne

- system, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 3 szt.
- Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2022 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, udziały sieciowe).
    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.

Dostarczone oprogramowanie musi być fabrycznie nowe.

7.7. Licencji dostępowych do systemu, na którym zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa

Wymagania ogólne

3. Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2022 Standard i w pkt. VII. wymagana dostarczenia licencji na oprogramowanie Microsoft Windows Server 2025 Standard lub nowszy lub równoważny serwerowy system operacyjny.
3. W ramach zamówienia Zamawiający wymaga dostarczenia licencji dostępowych CAL User dla 25 użytkowników lub równoważne licencje dostępowe dla oferowanego, równoważnego systemu operacyjnego.

7.8. Oprogramowanie SIEM (Security Information and Event Management)

Wymagania ogólne

- wdrożenie systemu typu opensource

Wymagania związane z rozwiązaniem SIEM:

1. System operacyjny powinien być na licencji Open Source (Ubuntu, Debian Linux 10, CentOS).
2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna.
3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source czyli MongoDB oraz Opensearch.
4. Tworzenie użytkowników w systemie centralnego składowania logów powinno odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
5. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów.
7. System centralnego składowania dzienników zdarzeń powinna udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
8. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
9. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
10. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia lub importowania listy z pliku do użycia w źródłach wejściowych.
11. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
12. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej.
13. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

14. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
15. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
16. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu.
17. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
18. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
19. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
20. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
21. Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.

7.9. Network Attached Storage (NAS)

Wymagania ogólne

- NAS 2 szt.

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

Nazwa elementu, parametru lub cechy	Opis wymagań
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 przesuwnymi umożliwiającymi montaż w szafie rack w zestawie.
Pamięć RAM	Minimum 8GB 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 16TB 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 1GbE RJ-45. • Minimum 2 porty 10GbE RJ-45. • Obsługa agregacji łączy.
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	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. 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. 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.
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.

7.10. System wirtualizacyjny dedykowany do systemów, na których zostanie zainstalowany produkt z zakresu cyberbezpieczeństwa

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 szeregowe.
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. Licencjonowanie nie może odbywać się w trybie OEM.
14. 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
15. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
16. Rozwiązanie powinno posiadać centralną konsolę do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
17. 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.
18. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
20. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
21. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych.
22. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
23. 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.
24. 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.

25. 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.
26. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
27. Należy dostarczyć licencję obsługującą 3 serwery po 2 procesory tak, aby licencja pozwalała na pełne wykorzystanie serwerów opisanych w pkt. 3.

7.11. Serwer do wykonywania kopii zapasowych

Wymagania ogólne

- serwer do backupu – 1 szt.

Minimalne wymagania do systemu backup:

Zarządzanie i magazyny

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2026 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. 28TB 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. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
12. 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).
13. 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.
14. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie.

15. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
16. 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.
17. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
18. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
19. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
20. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
21. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
22. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
23. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
24. 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.
25. 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.
26. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
27. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
28. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
29. 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).
30. 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.
31. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
32. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
33. 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.
34. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
35. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.

36. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
37. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
38. System musi pozwalać na automatyczne aktualizacje oprogramowania.
39. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
40. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
41. 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.
42. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
43. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
44. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
45. 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.
46. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
47. 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.
48. 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.
49. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
50. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
51. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
52. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
53. 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
54. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny
55. 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).
56. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami 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.
57. Możliwość generowania raportów dobowych w oparciu o harmonogram

58. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
59. 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)
60. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
61. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia 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+),
- Windows Server: 2008 R2+,

Środowiska wirtualne:

- 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 scalania 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 zastosowanie 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 zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
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).

1. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
2. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi.

3. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
4. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
5. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
6. System musi umożliwiać zabezpieczenie środowisk Jira.
7. 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

2. 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
2. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
2. 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.

System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

7.12. Oprogramowania do monitorowania infrastruktury informatycznej

Wymagania ogólne

- przedmiotem zamówienia jest usługa wdrożenia, konfiguracji oraz uruchomienia systemu monitorowania infrastruktury IT, opartego o oprogramowanie open source.

- wdrożone rozwiązanie musi zapewniać pełną funkcjonalność monitoringu infrastruktury IT bez konieczności ponoszenia dodatkowych kosztów licencyjnych po zakończeniu realizacji zamówienia.

Wymagania ogólne dotyczące rozwiązania

1. Rozwiązanie musi być oparte o oprogramowanie typu open source, dostępne na licencji umożliwiającej:
    - nieograniczone użytkowanie,
    - modyfikację,
    - dalszy rozwój we własnym zakresie,
    - brak opłat licencyjnych za monitorowane zasoby i użytkowników.
2. System musi być możliwy do zainstalowania na platformach Linux.
3. System musi posiadać graficzny interfejs użytkownika dostępny przez przeglądarkę internetową, bez konieczności instalowania dodatkowego oprogramowania klienckiego.
4. System musi umożliwiać pracę wielu jednoczesnych użytkowników z różnymi poziomami uprawnień.

Monitorowanie zasobów IT
System musi umożliwiać monitorowanie co najmniej:

1. serwerów fizycznych i wirtualnych,
2. systemów operacyjnych (Linux, Windows),
3. urządzeń sieciowych (przełączniki, routery, firewalle),
4. usług sieciowych i aplikacyjnych (HTTP/HTTPS, SMTP, DNS, LDAP, bazy danych),
5. zasobów sprzętowych (CPU, RAM, dyski, interfejsy sieciowe),
6. środowisk wirtualnych i kontenerowych (jeżeli występują u Zamawiającego).

Metody zbierania danych
System musi wspierać co najmniej następujące metody pozyskiwania danych:

1. agent instalowany na systemach monitorowanych,
2. protokół SNMP (v2c oraz v3),
3. monitorowanie bezagentowe,
4. monitorowanie usług sieciowych,
5. możliwość tworzenia własnych skryptów monitorujących.

Mechanizmy alarmowania
System musi zapewniać:

1. definiowanie progów alarmowych,
2. wielopoziomowe alarmy (warning, critical itp.),
3. eskalację alarmów,
4. powiadamianie co najmniej poprzez:
    - pocztę elektroniczną,
    - webhook / integrację z systemami zewnętrznymi,
5. możliwość definiowania harmonogramów powiadomień.

Wizualizacja i raportowanie

1. System musi oferować dashboardy prezentujące stan infrastruktury w czasie rzeczywistym.
2. System musi umożliwiać tworzenie:
    - wykresów historycznych,
    - map zależności infrastruktury,
    - widoków logicznych usług IT.
3. System musi umożliwiać eksport danych i raportów do formatów co najmniej:
    - CSV,

- PDF (lub równoważny).

Zarządzanie użytkownikami i uprawnieniami

1. System musi umożliwiać:
   - tworzenie użytkowników i grup użytkowników,
   - przypisywanie ról i zakresów dostępu,
   - integrację z usługą katalogową (np. LDAP/Active Directory).
2. Dostęp do zasobów i funkcjonalności systemu musi być kontrolowany w oparciu o nadane role.

Wymagania dotyczące wdrożenia
W ramach zamówienia Wykonawca zobowiązany jest do:

1. analizy infrastruktury Zamawiającego,
2. zaprojektowania architektury systemu monitoringu,
3. instalacji i konfiguracji systemu,
4. konfiguracji monitoringu kluczowych zasobów IT Zamawiającego,
5. konfiguracji mechanizmów alarmowania,
6. wykonania testów poprawności działania,
7. przekazania systemu do eksploatacji.

7.13. Wdrożenie oprogramowania z zakresu bezpieczeństwa – wdrożenie systemu typu opensource do analizy powłamaniowej;

Wymagania ogólne

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

Funkcjonalności wymagane
Oprogramowanie musi zapewniać co najmniej następujące funkcjonalności:
1. Obsługa obrazów danych
   a. Wczytywanie popularnych formatów obrazów dysków i partycji (m.in. E01, Ex01, AFF, RAW/dd).
   b. Obsługa obrazów urządzeń mobilnych i kopii logicznych (w miarę dostępności w narzędziu open source).
2. Analiza systemów plików
   a. Analiza systemów plików m.in. NTFS, FAT, exFAT, EXT, HFS+, APFS.
   b. Przeglądanie katalogów, metadanych, atrybutów plików.
   a. Wyszukiwanie usuniętych plików i katalogów.
3. Zaawansowane wyszukiwanie i indeksacja
   a. Automatyczna indeksacja zawartości plików.
   b. Wyszukiwanie słów kluczowych także w plikach zagnieżdżonych (archiwa, dokumenty).
   c. Obsługa wyrażeń regularnych.
4. Analiza artefaktów systemowych
Oprogramowanie musi posiadać moduły umożliwiające analizę m.in.:
   a. historii przeglądarek internetowych,
   b. plików dzienników systemowych,
   c. rejestru systemowego,
   d. list ostatnio otwieranych plików,
   e. konfiguracji systemowych i użytkownika,

f. historii połączeń sieciowych.

5. Analiza danych multimedialnych
   a. Przeglądanie obrazów, video, audio.
   b. Wykrywanie plików o określonych sygnaturach (file carving).
   c. Rozpoznawanie metadanych (EXIF i inne).
6. Raportowanie
   a. Generowanie raportów w formatach PDF/HTML/CSV.
   b. Możliwość tworzenia zestawień i eksportowania wyników analizy.
   c. Oznaczanie znalezionych artefaktów jako dowody.
7. Praca z wieloma przypadkami
   a. Tworzenie wielu projektów dochodzeniowych.
   b. Oddzielne przechowywanie wyników analizy.
   c. 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).

7.14. System MFA

Wymagania ogólne

- Zamawiający korzysta zrozwiązań Fortinet i wymaga dostarczenia licencji na FortiToken Mobile dla 25 użytkowników.

Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego względem produktu FortiToken Mobile, pod warunkiem spełnienia co najmniej poniższych wymagań funkcjonalnych, technicznych i licencyjnych:

1. Oferowane rozwiązanie musi stanowić programowy token jednorazowych haseł (Software OTP Token) przeznaczony do realizacji uwierzytelniania wieloskładnikowego (MFA).
2. Rozwiązanie musi umożliwiać generowanie haseł jednorazowych w standardzie:
   - HOTP i/lub
   - TOTP zgodnym z OATH.
3. Oferowane rozwiązanie musi być dostępne co najmniej dla następujących platform:
   - iOS,
   - Android,
   - Windows.
4. Aplikacja kliencka musi umożliwiać generowanie kodów OTP bez konieczności stałego dostępu do sieci Internet lub sieci komórkowej po wcześniejszej aktywacji tokena.
5. Rozwiązanie musi umożliwiać centralne zarządzanie tokenami z poziomu urządzenia lub systemu uwierzytelniającego producenta.
6. Licencja musi umożliwiać przypisanie tokenów do określonej liczby użytkowników wskazanej w OPZ.
7. Licencja musi być przypisywana do pojedynczego urządzenia/appliance producenta systemu uwierzytelniającego i nie może umożliwiać swobodnego transferu pomiędzy różnymi urządzeniami bez udziału producenta lub jego wsparcia technicznego.
8. Rozwiązanie musi umożliwiać:
   - aktywację tokena przy użyciu kodu aktywacyjnego lub kodu QR,

- ponowną aktywację tokena użytkownika w przypadku wymiany urządzenia mobilnego.

9. Oferowane rozwiązanie musi wspierać integrację co najmniej z:
    - urządzeniami klasy firewall/VPN,
    - systemami uwierzytelniania i kontroli dostępu,
    - usługami zdalnego dostępu VPN.
10. Rozwiązanie musi zapewniać bezpieczne przechowywanie sekretów kryptograficznych/tokenów oraz szyfrowanie danych używanych do generowania OTP.
11. Oferowane rozwiązanie musi pochodzić z oficjalnego kanału dystrybucji producenta oraz posiadać wsparcie producenta zgodne z wymaganiami określonymi w OPZ.
12. W przypadku zaoferowania rozwiązania równoważnego Wykonawca zobowiązany jest wykazać równoważność poprzez dostarczenie dokumentacji producenta potwierdzającej spełnienie wszystkich wymaganych funkcjonalności.

7.15. Szafy RACK do produktów i rozwiązań z zakresu bezpieczeństwa

Wymagania ogólne

1. Szafy RACK do produktów i rozwiązań z zakresu bezpieczeństwa - 1 szt.
2. Oferowany sprzęt musi być fabrycznie nowy i nieużywany przed dniem dostarczenia do siedziby Zamawiającego.
3. Data produkcji nie może być wcześniejsza niż 2025 rok.

Minimalne wymagania techniczne:

1. typ szafy: wolnostojąca
2. pojemność stelaża: 42U
3. szerokość: 600mm
4. głębokość: 1000mm
5. maksymalna waga przeznaczona do umieszczenia/przechowywania przez urządzenie: 1500 kg
6. materiał wykonania: stal
7. rodzaj ramy: zamknięty
8. konstrukcja drzwi tylnych: metal
9. konstrukcja drzwi przednich: szkło hartowane
10. zdejmowalne drzwi tylne
11. zdejmowalne drzwi przednie
12. zdejmowalne panele boczne
13. regulowane wymiary wejść kablowych na pokrywę górną i płytę dolną
14. możliwość otwierania drzwi na lewą lub prawą stronę
15. zamek
16. zamek klucza drzwi przednich
17. zamek na klucz panelu bocznego
18. relingi
19. regulowane nóżki (stopy)

7.16. Oprogramowanie do zarządzania podatnościami

1. Przedmiot zamówienia

Wymagania ogólne

1. Przedmiotem zamówienia jest dostawa licencji, wdrożenie, konfiguracja oraz uruchomienie systemu do zarządzania podatnościami infrastruktury teleinformatycznej Zamawiającego.
2. System ma umożliwiać identyfikację podatności, ocenę poziomu ryzyka, monitorowanie stanu bezpieczeństwa zasobów oraz raportowanie wyników.

Wymagania funkcjonalne

Oferowane rozwiązanie musi umożliwiać:

1. Identyfikację podatności w:
    - systemach operacyjnych Microsoft Windows,
    - systemach Linux,
    - urządzeniach sieciowych,
    - urządzeniach wirtualnych,
    - urządzeniach końcowych.
2. Skanowanie:
    - z wykorzystaniem poświadczeń administracyjnych,
    - bez wykorzystania poświadczeń,
    - z użyciem agentów instalowanych na urządzeniach końcowych, lub równoważnego mechanizmu.
3. Definiowanie harmonogramów skanowania oraz uruchamianie skanowania na żądanie.
4. Automatyczne wykrywanie nowych zasobów w monitorowanym środowisku.
5. Grupowanie zasobów według definiowanych kryteriów, w szczególności:
    - adresów IP,
    - nazw hostów,
    - systemów operacyjnych,
    - lokalizacji,
    - tagów, atrybutów, filtrów lub zapytań.
6. Automatyczne przypisywanie zasobów do grup zgodnie z określonymi regułami.

Zarządzanie podatnościami

System musi:

1. Korzystać z aktualnej bazy podatności aktualizowanej przez producenta.
2. Identyfikować podatności zgodnie z publicznie dostępnymi bazami podatności, w szczególności wykorzystując identyfikatory CVE.
3. Określać poziom ryzyka wykrytych podatności z wykorzystaniem standardu CVSS w wersji co najmniej 3.0.
4. Uwzględniać przy priorytetyzacji podatności informacje dotyczące:
    - poziomu zagrożenia,
    - dostępności exploitów,
    - możliwości wykorzystania podatności,
    - wpływu podatności na bezpieczeństwo zasobu.
5. Umożliwiać filtrowanie wyników według:
    - poziomu krytyczności,
    - identyfikatora CVE,
    - systemu operacyjnego,
    - typu urządzenia,
    - daty wykrycia,
    - statusu podatności.
6. Przechowywać historię wykrytych podatności oraz umożliwiać porównywanie wyników kolejnych skanowań.
7. Wskazywać rekomendowane działania naprawcze dla wykrytych podatności.

Raportowanie

System musi umożliwiać:

1. Tworzenie raportów obejmujących:
    - wykryte podatności,
    - poziom ryzyka,
    - trendy zmian,
    - podatności krytyczne,
    - stan bezpieczeństwa poszczególnych grup zasobów.
2. Eksport raportów do co najmniej formatów:
    - PDF, lub HTML,
    - oraz do formatu umożliwiającego dalsze przetwarzanie danych, np. CSV, XLSX, XML lub JSON.
3. Automatyczne generowanie raportów zgodnie z harmonogramem.
4. Udostępnianie interaktywnych paneli prezentujących aktualny poziom bezpieczeństwa.

Zarządzanie użytkownikami
System musi:
1. Obsługiwać wielu użytkowników.
2. Umożliwiać definiowanie ról oraz uprawnień.
3. Rejestrować działania administratorów w dzienniku zdarzeń.
4. Umożliwiać integrację z usługą katalogową LDAP lub Active Directory albo innym rozwiązaniem zgodnym z LDAP.

Integracja
System powinien umożliwiać:
1. Integrację z systemami SIEM poprzez interfejs API.
2. Integrację z systemami zgłoszeniowymi (Service Desk) z wykorzystaniem interfejsu REST API, eksport danych, konektor producenta, albo możliwość generowania ticketów w systemie..
3. Eksport danych do zewnętrznych systemów analitycznych.

Wymagania techniczne
1. Rozwiązanie może być oferowane w modelu chmurowym (SaaS) lub lokalnym (on-premise).
2. Komunikacja z systemem musi odbywać się z wykorzystaniem szyfrowania TLS.
3. Aktualizacja bazy podatności musi odbywać się automatycznie.
4. System musi umożliwiać jednoczesną pracę co najmniej trzech administratorów.
5. Interfejs administracyjny musi być dostępny z poziomu przeglądarki internetowej.

Licencjonowanie
1. Licencja musi obejmować monitorowanie minimum 100 aktywów.
2. Licencja musi zapewniać dostęp do wszystkich aktualizacji oprogramowania oraz bazy podatności przez cały okres obowiązywania umowy.
3. W okresie obowiązywania licencji nie mogą występować ograniczenia liczby wykonywanych skanowań.

Wdrożenie
Wykonawca zobowiązany będzie do:
1. konfiguracji rozwiązania,
2. uruchomienia skanowania,
3. konfiguracji harmonogramów,
4. konfiguracji raportów.

8. Bezpieczeństwo prac Wykonawcy

8.1. Dostęp do środowiska Zamawiającego

Dostęp Wykonawcy do środowiska Zamawiającego może odbywać się wyłącznie w zakresie i czasie niezbędnym do realizacji zamówienia oraz po uzgodnieniu z Zamawiającym.

Wykonawca zobowiązany jest do:

1. wskazania osób uprawnionych do dostępu,
2. korzystania z imiennych kont administracyjnych, o ile jest to możliwe,
3. stosowania MFA dla dostępów zdalnych, o ile jest to technicznie możliwe,
4. rejestrowania działań administracyjnych,
5. korzystania z szyfrowanych kanałów komunikacji,
6. niezwłocznego zgłaszania incydentów lub podejrzeń incydentów,
7. usunięcia lub dezaktywacji dostępów po zakończeniu prac.
8. prowadzenia prac w uzgodnionych oknach serwisowych, jeżeli dana czynność może wpływać na dostępność lub bezpieczeństwo środowiska Zamawiającego,
9. uzgadniania z Zamawiającym czynności mogących powodować przerwy, degradację usług, zmianę reguł komunikacji, zmianę polityk bezpieczeństwa, restart komponentów lub zmianę konfiguracji styku IT/OT,
10. przywrócenia lub wycofania zmiany w przypadku niepowodzenia, jeżeli jest to technicznie możliwe i zostało przewidziane w planie realizacji,
11. niepogarszania bezpieczeństwa, dostępności ani ciągłości działania środowiska OT oraz styków IT/OT Zamawiającego,
12. przekazania Zamawiającemu informacji o wszystkich kontach, poświadczeniach, kluczach, tokenach, dostępach tymczasowych i mechanizmach zdalnego dostępu wykorzystywanych w trakcie realizacji zamówienia.

8.2. Poufność i ochrona informacji

Wykonawca jest zobowiązany do zachowania poufności informacji uzyskanych w związku z realizacją zamówienia, w szczególności informacji dotyczących infrastruktury IT/OT, konfiguracji, zabezpieczeń, kont, podatności, incydentów, dokumentacji technicznej oraz organizacji pracy Zamawiającego.

9. Wymagania dotyczące oferty i dowodów zgodności

9.1. Przedmiotowe środki dowodowe

W celu potwierdzenia zgodności oferowanego rozwiązania z OPZ Wykonawca jest zobowiązany przedłożyć, w zakresie wymaganym przez Zamawiającego:

1. karty katalogowe,
2. opisy techniczne,
3. dokumentację producenta,
4. oświadczenia producenta lub autoryzowanego dystrybutora,
5. certyfikaty, jeżeli są wymagane,
6. potwierdzenie legalności licencji,
7. potwierdzenie okresów wsparcia,
8. potwierdzenie dostępności aktualizacji,
9. wykaz oferowanych komponentów,
10. opis architektury proponowanego rozwiązania,
11. opis sposobu spełnienia wymagań równoważności, jeżeli dotyczy.
12. potwierdzenie pochodzenia sprzętu, oprogramowania, licencji, subskrypcji i usług wsparcia z oficjalnego kanału dystrybucji producenta lub autoryzowanego dystrybutora,
13. potwierdzenie, że oferowane produkty nie są wycofane ze sprzedaży, nie są przeznaczone wyłącznie do odsprzedaży poza Europejskim Obszarem Gospodarczym i mogą być legalnie użytkowane przez Zamawiającego w Polsce,
14. potwierdzenie zakresu i okresu obowiązywania licencji, subskrypcji, wsparcia, aktualizacji, baz sygnatur, reguł detekcyjnych i gwarancji dla każdego komponentu, którego to dotyczy.

9.2. Wykaz oferowanych komponentów

Wykonawca jest zobowiązany przedstawić wykaz oferowanych komponentów i tabelę zgodności obejmujący co najmniej:

1. nazwę komponentu,
2. producenta,
3. model lub nazwę handlową,
4. wersję,
5. liczbę sztuk lub licencji,
6. okres licencji,
7. okres gwarancji,
8. okres wsparcia,
9. informację o sposobie wdrożenia,
10. informację o zależnościach licencyjnych lub subskrypcyjnych.
11. informację o kanale dystrybucji,
12. informację o sposobie aktualizacji,
13. informację o ograniczeniach licencyjnych, subskrypcyjnych lub wdrożeniowych,
14. informację, czy dany komponent wymaga połączenia z chmurą producenta, usługą zewnętrzną lub kontem producenta,
15. informację o rodzaju i okresie wsparcia oraz podmiocie świadczącym wsparcie.

10. Harmonogram realizacji

1. Wykonawca zobowiązany jest zrealizować całość zamówienia w terminie określonym w IDW i umowie, nie później niż do dnia 30.11.2026 r.
2. Szczegółowy harmonogram zostanie przedstawiony przez Wykonawcę w planie realizacji i będzie wymagał akceptacji Zamawiającego.
   Harmonogram powinien przewidywać co najmniej:
   a. analizę przedwdrożeniową,
   b. dostawy,
   c. instalację,
   d. konfigurację,
   e. integrację,
   f. hardening,
   g. testy,
   h. szkolenie,
   i. odbiory cząstkowe,
   j. odbiór końcowy,
   k. okres stabilizacji i wsparcia powdrożeniowego, jeżeli jest przewidziany przed zakończeniem realizacji zamówienia.

Harmonogram powinien uwzględniać okna serwisowe, etapowanie prac, zależności od działań Zamawiającego, odbiory cząstkowe oraz sposób zarządzania ryzykami wpływającymi na ciągłość działania środowiska IT/OT.

11. Kryteria odbioru końcowego

Rozwiązanie zostanie uznane za wykonane prawidłowo, jeżeli:

1. wszystkie komponenty objęte zamówieniem zostały dostarczone,
2. dostarczone komponenty są zgodne z ofertą i OPZ,
3. rozwiązanie zostało zainstalowane i uruchomione,
4. wykonano wymagane konfiguracje i integracje,
5. wykonano hardening,
6. wykonano testy z wynikiem pozytywnym,

7. przekazano wymaganą dokumentację,
8. przeprowadzono szkolenie,
9. przekazano licencje, dostęp administracyjny i informacje gwarancyjne,
10. Zamawiający otrzymał komplet protokołów,
11. nie występują błędy krytyczne uniemożliwiające eksploatację rozwiązania,
12. potwierdzono wykonanie integracji z SIEM, monitoringiem, AD, backupem, UTM, XDR, NAC, MFA oraz pozostałymi komponentami przewidzianymi w architekturze wdrożenia,
13. potwierdzono wykonanie testów odtworzeniowych i przekazanie procedur odtwarzania,
14. potwierdzono usunięcie, dezaktywację albo ograniczenie dostępów Wykonawcy do środowiska Zamawiającego,
15. potwierdzono przekazanie informacji o gwarancji, wsparciu, kanałach zgłoszeń, licencjach, subskrypcjach, aktualizacjach i ograniczeniach licencyjnych.