SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
POSTĘPOWANIE PODZIELONE NA 2 CZĘŚCI

Projekt: „Podniesienie poziomu bezpieczeństwa cybernetycznego poprzez modernizację i zabezpieczenie infrastruktury teleinformatycznej budynku administracyjnego”

Zamawiający: Miasto i Gmina Solec nad Wisłą

Niniejszy dokument stanowi opis przedmiotu zamówienia dla postępowania podzielonego na dwie części. Wykonawca może złożyć ofertę na jedną część albo na obie części, zgodnie z dokumentacją postępowania.

I. Podział zamówienia na części

Część	Nazwa części	Zakres podstawowy
Część 1	Dostawa, montaż, instalacja, konfiguracja i uruchomienie infrastruktury sprzętowej, sieciowej, systemu bezpieczeństwa UTM oraz ochrony antywirusowej z EDR	Serwer z szafą RACK i UPS, oprogramowanie antywirusowe z EDR, urządzenia sieciowe, segmentacja sieci, macierz dyskowa z dyskami, system bezpieczeństwa UTM wraz z oprogramowaniem i licencjami.
Część 2	Zakres organizacyjno-kompetencyjny oraz zintegrowane środowisko oprogramowania cyberbezpieczeństwa	Dokumentacja SZCD/BCP/DRP, audyt, doradztwo w zakresie opracow. warunków umów kontraktowych na wdrożenie z usługami wspomagającymi realizację projektu, szkolenia i testy socjotechniczne oraz środowisko oprogramowania cyberbezpieczeństwa obejmujące m.in. backup, menadżer logów/SIEM, XDR, ochronę poczty, DLP i wirtualizację.

Szczegółowe wymagania techniczne dla Części 1 i Części 2 określono w dalszej części dokumentu.

CZĘŚĆ 1 – OPIS PRZEDMIOTU ZAMÓWIENIA

Poniżej znajduje się specyfikacja techniczna Części 1

Przedmiot zamówienia:

1 . Zakup i dostawa serwera wraz z szafą RACK oraz UPS – 1 kpl.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa typu RACK o wysokości max. 3U wyposażony w szyny ruchome oraz elementy do montażu w szafie serwerowej
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta serwera, trwale oznaczona (na laminacie płyty głównej) z nazwą producenta oferowanego serwera i dedykowana dla danego urządzenia. Płyta główna powinna umożliwiać zainstalowanie 2 procesorów oraz pamięci RAM
Procesor	Zainstalowane min. minimum 1 procesor przeznaczony do pracy ciągłej (serwerowy) o architekturze x86-64 / x64, minimum 16 rdzeni / 32 wątki, taktowanie bazowe minimum 2,00 GHz, pamięć cache minimum 30 MB, obsługa PCIe 5.0 lub równoważny wydajnościowo
RAM	Minimum 64 GB DDR5 ECC RDIMM z możliwością rzbudowy
Interfejsy sieciowe/FC/SAS	Wbudowana w płytę główną dwu portowa karta sieciowa z min. 2 portami 1Gbit/s. Dodatkowo zainstalowana dwu portowa karta 10Gbit/s SFP+. Interfejsy sieciowe muszą pochodzić od tego samego producenta.
Dyski twarde	Zainstalowane min. 6 dysków SAS, każdy o pojemności min. 2,4 TB o parametrach interfejs 12 Gb/s , funkcja szybkiego, bezpiecznego usuwania danych z dysku przez unieważnienie/usunięcie klucza szyfrowania danych; wymienne bez wyłączania systemu Uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 12 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10 Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	Minimum USB, VGA, dedykowany port zarządzania, porty sieciowe, możliwość zdalnego zarządzania.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Zasilacze	2 zasilacze o mocy co najmniej 1100W, redundancyjne, dedykowane do zaoferowanego sprzętu zwymiarowane do wewnętrznych podzespołów, wymienne bez wyłączania systemu
Szafa RACK	W komplecie do oferowanego sprzętu wszystkie niezbędne do uruchomienia kable zasilające, przewody sygnałowe wraz z szafą szafa rack 19” 42U 600x1200.
Diagnostyka	Serwer musi być dostarczony z przednim panelem diagnostycznym LCD, umożliwiającym wyświetlanie informacji o stanie systemu, komunikatów błędów oraz podstawowych informacji diagnostycznych, w tym informacji dotyczących stanu systemu, zasilania, temperatury oraz adresu IP kontrolera zarządzania.
SFP+	Moduł SFP (3 kpl.) – 3 sztuki : wielomodowy, dupleksowy, światłowodowy moduł nadawczo-odbiorczy optyczny SFP+ ; Obsługiwane multimedia: Światłowód wielomodowy;Typ złącza: 2x LC; Prędkość transmisji danych 10 Gb/s na odległość do min. 300 metrów;
Karta Zarządzania	Zintegrowany kontroler zdalnego dostępu umożliwiający administratorom monitorowanie, zarządzanie, aktualizowanie, rozwiązywanie problemów i naprawę z dowolnego miejsca i bez użycia agentów. Niezależnie od obecności lub stanu systemu operacyjnego, hiperwizora lub

	monitora maszyn wirtualnych.
Certyfikaty	Certyfikat ISO 9001:2015 oraz 27001:2023 wykonawcy na dostarczanie usług serwisowych do urządzeń oraz wdrożeń systemów Wykonawca, zobowiązany jest załączyć wymagany certyfikat do oferty.
Warunki gwarancji	Serwer z co najmniej 36 miesięczną gwarancją, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 3 godzin roboczych w godzinach pracy Zamawiającego tj.: Poniedziałek - Piątek: 7:00 - 15:00. Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
UPS Rack	1 sztuka UPS Typ Online, Technologia online/VFI, rack/tower 19″ 2U; min. 2000 VA / 1800 W; pełna sinusoida; czas przełączenia 0 ms; wewnętrzne akumulatory min. 6× 12 V/9 Ah; min. 2× Schuko; LCD, USB, RS-232, EPO; zestaw do montażu rack; urządzenie z wbudowanymi akumulatorami.
Instalacja, konfiguracja i uruchomienie sprzętu	W ramach postępowania wraz z dostawą wykonana zostanie instalacja, podłączenie oraz konfiguracja i uruchomienie sprzętu wraz z migracją danych z obecnego systemu posiadanego przez Zamawiającego. • Montaż fizycznych składników rozwiązania, podłączenie i konfiguracja interfejsów sieciowych, konfiguracja interfejsów zarządzających serwerami, aktualizacja oprogramowania sprzętowego. • Konfiguracja urządzeń sieciowych w odniesieniu do rozwiązania wirtualizacyjnego, • Instalacja systemów operacyjnych (np. serwer Windows), aktualizacja. • Konfiguracja usługi bazującej na oprogramowaniu definiowanym magazynem. • Konfiguracja usług klastra dotyczących wirtualizacji, definiowanie sieci wirtualnych, • Instalacja i konfiguracja maszyn wirtualnych (np. serwer Windows). • Tworzenie wzorcowego obrazu maszyny wirtualnej (np. serwer Windows). • Instalacja oprogramowania do zarządzania kopiami zapasowymi na dedykowanym serwerze, konfiguracja lokalnych zasobów serwera jako repozytorium kopii zapasowych, konfiguracja zadań tworzenia kopii zapasowych dla danego środowiska, weryfikacja kopii zapasowej - przywrócenie wybranej maszyny • Konfiguracja serwera VPN • Migracją danych z obecnego systemu posiadanego przez Zamawiającego wraz z obecnie wykorzystywanym oprogramowaniem. • Weryfikacja funkcjonowania środowiska. • Włączenie funkcji serwera usług katalogowych na wybranej maszynie wirtualnej. • Konfiguracja polityk usług katalogowych dotyczących urządzeń i użytkowników. • Konfiguracja profili użytkowników. • Konfiguracja dostępu do wybranych zasobów. • Instalacja usług serwera terminalowego na maszynie wirtualnej i konfiguracja usług zdalnego dostępu dla użytkowników. • Konfiguracja dostępu terminalowego na wszystkich hostach(komputerach klienckich) • Migracja obecnych profili użytkowników do serwera terminalowego

	• Konfiguracja połączeń VPN dla dostępów zdalnych na urządzeniach mobilnych

2 . Oprogramowanie antywirusowe z EDR

Aktualnie w w ramach struktur zamwiającego wykorzystywane jest oprogramowanie antywirusowe (ochrona stacji roboczych, urządzeń mobilnych, wirtualnych stacji mobilnych ESET). Wykonawca musi mieć wdrożony oraz stosować zintegrowany system zarządzania jakością i bezpieczeństwem informacji zgodny z wymaganiami norm ISO 9001 oraz 27001 minimum w zakresie wdrożeń systemów informatycznych oraz oprogramowania. Dostarczone rozwiązanie musi zapewniać kompleksową ochronę z EDR zapobiegającą naruszeniom bezpieczeństwa do 31.12.26 r., oraz musi mieć możliwość jednoczesnej pracy dla 33 stanowisk wykorzystywanej przez urząd oraz spełniać niżej określone minimalne wymogi funkcjonalne.

Wymagane minimalne parametry techniczne
Administracja zdalna • Konsola centralnego zarządzania jest dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS). • Rozwiązanie umożliwia dostęp do konsoli centralnego zarządzania z poziomu interfejsu www. • Rozwiązanie jest zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS. • Rozwiązanie posiada mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. Rozwiązanie posiada dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą: Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania, Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta, Buforowanie ruchu HTTPS. Rozwiązanie posiada możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. Rozwiązanie posiada możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej. Uwierzytelnianie dwuskładnikowe jest realizowane przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android: Google Authenticator, Microsoft Authenticator, Authy, Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania. adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania oraz ochrony, wersja systemu operacyjnego, podzespoły komputera. wyrażenie CRON, codziennie, cotygodniowo, co miesiąc, co rok, po wystąpieniu nowego zdarzenia, po automatycznym umieszczeniu hosta w grupie dynamicznej.

1. Rozwiązanie posiada minimum 80 szablonów raportów, przygotowanych przez producenta.
2. Rozwiązanie posiada możliwość tworzenia grup statycznych i dynamicznych komputerów.
3. Grupy dynamiczne są tworzone na podstawie szablonu określającego warunki, jakie komputer musi spełnić, aby został umieszczony w danej grupie. Warunki zawierają:
4. Rozwiązanie posiada możliwość uruchomienia zadań automatycznie oraz z wyzwalaczem:

    1. Konsola centralnego zarządzania jest dostępna w języku polskim oraz angielskim.
    2. Język konsoli centralnego zarządzania jest możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania.
    3. Rozwiązanie ma możliwość tagowania obiektów.
    4. Rozwiązanie posiada możliwość eksportu danych do zewnętrznych systemów, w tym Syslog.

Eksport danych jest możliwy w następujących formatach: JSON,
LEEF,
CEF.

Rozwiązanie ma możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w systemie centralnego zarządzania.

Ochrona stacji roboczych - Windows

1. Rozwiązanie wspiera systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie jest dostępne w języku polskim oraz angielskim.
3. Rozwiązanie zapewnia wykrywanie i usuwanie zagrożeń typu:
4. wirus,
5. trojan,
6. robak,

    1. adware,
    2. spyware,
    3. dialer,
    4. phishing,
    5. backdoor.
    6. Rozwiązanie zapewnia wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
    7. Rozwiązanie posiada wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
    8. Rozwiązanie posiada ochronę przed podłączeniem hosta do sieci botnet.
    9. Rozwiązanie posiada funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
    10. Technologia ta jest autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
    11. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie wykorzystuje mechanizmu VSS (Volume Shadow Copy Service).
    12. Technologia, która tworzy kopię zapasową plików działa w czasie rzeczywistym i zabezpiecza pliki przed modyfikacją przez podejrzane procesy.
    13. Rozwiązanie zapewnia wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
    14. Rozwiązanie zapewnia skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
    15. Rozwiązanie zapewnia skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem :
    16. całego dysku,

17. wybranych katalogów,
18. pojedynczych plików,

1. plików spakowanych oraz skompresowanych,
2. dysków sieciowych,
3. dysków przenośnych.
4. Rozwiązanie posiada opcję umieszczenia na liście wykluczeń ze skanowania :
5. wybranych plików,
6. wybranych procesów,
7. wybranych lokalizacji,
8. wybranych rozszerzeń,
9. nazwy wykrycia,
10. sumy kontrolnej (SHA1).
11. Rozwiązanie integruje się z Intel Threat Detection Technology.
12. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia :
13. Sprawdzenie reputacji działających procesów i plików z poziomu interfejsu programu oraz menu kontekstowego.
14. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
15. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
16. Rozwiązanie zapewnia 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).

1. Rozwiązanie zapewnia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
2. Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie -- z użyciem jednej lub obu metod jednocześnie.
3. Rozwiązanie zapewnia blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o :
4. typ urządzenia:
5. pamięci masowe,
6. optyczne pamięci masowe,
7. pamięci masowe Firewire,
8. urządzenia do tworzenia obrazów,
9. drukarki USB,
10. urządzenia Bluetooth,
11. czytniki kart inteligentnych,
12. modemy,
13. porty LPT/COM,
14. urządzenia przenośne.
15. parametry urządzenia:
16. numer seryjny,

1. producent,
2. model.
3. typ dostępu:
4. brak możliwości zapisu,

5. pełen dostęp,
6. ostrzeżenie użytkownika,
7. brak dostępu.
8. Moduł HIPS posiada możliwość pracy w jednym z pięciu trybów:
9. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje
10. reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
11. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku
12. wykrycia aktywności w systemie,
13. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez

użytkownika,

1. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program samoczynnie przełącza się w tryb pracy oparty na regułach,
2. tryb inteligentny, w którym rozwiązanie powiadamia wyłącznie o szczególnie podejrzanych zdarzeniach.
3. Rozwiązanie jest wyposażone we wbudowaną funkcję, która generuje pełny raport na temat stacji.

1. Funkcja, generująca taki log, posiada przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
2. Istnieje możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
3. Raport posiada :
4. Listę zainstalowanych aplikacji,
5. Listę usług systemowych,
6. Informacje o systemie operacyjnym i sprzęcie,
7. Listę aktywnych procesów i połączeń sieciowych,
8. Harmonogram systemu operacyjnego,
9. Szczegóły pliku hosts,
10. Informacje o sterownikach.
11. Rozwiązanie posiada tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają następujące funkcje systemu:
12. antywirus,
13. zapora osobista
14. sandbox,
15. antyspyware,
16. metody heurystyczne.

1. Rozwiązanie posiada funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
2. Rozwiązanie posiada ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
3. Wtyczka ta jest dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
4. Ochrona jest realizowana w oparciu o :
5. globalna czarna lista RBL,
6. czarna lista użytkownika,
7. biała lista użytkownika, na którą automatycznie zostają dodane adres email z książki adresowej klienta Microsoft Outlook.
8. Rozwiązanie posiada wbudowany system IDS, który posiada następujące funkcjonalności:
9. Ochrona przed anomaliami sieciowymi, w tym :
10. Skanowanie portów TCP oraz UDP,
11. Wykrywanie duplikacji adresu IP,
12. Atak zatruwania ARP,

13. Nieprawidłowa długość pakietu TCP oraz UDP.
14. Ochrona przed atakami typu brute-force dla usług oraz protokołów:
15. RDP,
16. SMB,
17. My SQL,

1. MS SQL.
2. Możliwość dodawania wyjątków dla systemu IDS, w oparciu o występujący alert,
3. kierunek, aplikacje, czynność oraz adres IP.
4. Rozwiązanie posiada moduł zapory osobistej, która pochodzi od tego samego producenta antywirusowego.
5. Zapora osobista działa w oparciu o reguły i posiada 60 wbudowanych reguł, stworzonych przez producenta.
6. Zapora osobista posiada cztery tryby pracy:
7. tryb automatyczny -- rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
8. tryb interaktywny -- rozwiązanie pyta się o każde nowo nawiązywane połączenie,
9. tryb oparty na regułach -- rozwiązanie blokuje ruch przychodzący i wychodzący,
10. tryb uczenia się -- rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator posiada możliwość skonfigurowania czasu działania trybu.
11. Rozwiązanie posiada moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
12. Bezpieczna przeglądarka automatycznie szyfruje wszelkie dane wprowadzane przez Użytkownika.
13. Praca w bezpiecznej przeglądarce jest wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
14. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki ulega zmianie oraz pojawia się alert informujący o zdalnym połączeniu.
15. Rozwiązanie jest wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
16. Rozwiązanie posiada możliwość filtrowania adresów URL w oparciu o 160 kategorii i podkategorii.

1. Rozwiązanie umożliwia stworzenie własnego komunikatu na zablokowanych stronach w oparciu o :
2. Treść komunikatu,
3. Obraz.

Ochrona stacji roboczych - macOS

1. Rozwiązanie posiada pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie jest dostępne w języku polskim oraz angielskim.
3. Rozwiązanie zapewnia wykrywanie i usuwanie zagrożeń typu:
4. wirus,
5. trojan,
6. robak,
7. adware,
8. spyware,
9. dialer,
10. phishing,
11. backdoor.

1. Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie -- z użyciem jednej lub obu metod jednocześnie.

2. Rozwiązanie posiada możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
3. Rozwiązanie chroni pliki za pomocą:
4. Sygnatur wirusów.
5. Reputacji chmurowej.
6. Rozwiązanie umożliwia 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).
7. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia :
8. Sprawdzenie reputacji działających aplikacji i plików z poziomu interfejsu programu.
9. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
10. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
11. Rozwiązanie zapewnia skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem :
12. całego dysku,
13. wybranych katalogów,
14. pojedynczych plików,

1. plików spakowanych oraz skompresowanych,
2. Dysków sieciowych,
3. dysków przenośnych.
4. Rozwiązanie posiada opcję umieszczenia na liście wykluczeń ze skanowania :
5. wybranych plików,
6. wybranych procesów,
7. wybranych lokalizacji,
8. wybranych rozszerzeń,
9. nazwy wykrycia,
10. sumy kontrolnej (SHA1).
11. Rozwiązanie posiada moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
12. Zapora osobista działa w oparciu o reguły i posiada 30 wbudowanych reguł, stworzonych przez producenta.
13. Zapora osobista posiada dwa tryby pracy:
14. tryb automatyczny -- rozwiązanie blokuje ruch przychodzący i zezwala tylko
15. na połączenia wychodzące,
16. tryb oparty na regułach -- rozwiązanie blokuje ruch przychodzący i wychodzący.

Ochrona stacji roboczych - Linux

1. Rozwiązanie wspiera następujące systemy operacyjne:
2. Ubuntu Desktop,
3. Red Hat Enterprise Linux
4. Linux Mint.
5. Rozwiązanie obsługuje następujące środowiska pulpitu:
6. Cinnamon,
7. GNOME,
8. KDE,
9. MATE,
10. XFCE.
11. Rozwiązanie zapewnia wykrywanie i usuwanie zagrożeń typu:
12. wirus,
13. trojan,
14. robak,
15. adware,

16. spyware,

1. dialer,
2. phishing,
3. backdoor.
4. Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie -- z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie posiada możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia :
7. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
8. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie zapewnia skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem :
10. całego dysku,
11. wybranych katalogów,
12. pojedynczych plików,
13. plików spakowanych oraz skompresowanych,
14. dysków sieciowych,
15. dysków przenośnych.

1. Rozwiązanie posiada opcję umieszczenia na liście wykluczeń ze skanowania :
2. wybranych plików,
3. wybranych procesów,
4. wybranych lokalizacji,
5. wybranych rozszerzeń.
6. Rozwiązanie zapewnia blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o :
7. typ urządzenia:
8. pamięci masowe,
9. optyczne pamięci masowe,
10. parametry urządzenia: o numer seryjny, o producent, o model.
11. typ dostępu:
12. brak możliwości zapisu,
13. pełen dostęp,
14. brak dostępu.

Ochrona serwera - Windows Server

1. Rozwiązanie wspiera systemy w tym :
2. Microsoft Windows Server 2012 R2,

1. Microsoft Windows Server 2016,
2. Microsoft Windows Server 2019,
3. Microsoft Windows Server 2022,
4. Microsoft Windows Server 2025.
5. Rozwiązanie zapewnia ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Rozwiązanie zapewnia wykrywanie i usuwanie zagrożeń typu:
7. wirus,
8. trojan,

9. robak,
10. adware,
11. spyware,
12. dialer,
13. phishing,
14. backdoor.
15. Rozwiązanie zapewnia możliwość skanowania dysków sieciowych typu NAS.
16. Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Istnieje możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie -- z użyciem jednej lub obu metod jednocześnie.

1. Rozwiązanie wspiera automatyczną, inkrementacyjną aktualizację silnika detekcji.
2. Rozwiązanie posiada możliwość wykluczania ze skanowania procesów.
3. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia :
4. Sprawdzenie reputacji działających procesów i plików z poziomu interfejsu programu oraz menu kontekstowego.
5. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
6. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
7. Rozwiązanie zapewnia skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem :
8. całego dysku,
9. wybranych katalogów,
10. pojedynczych plików,
11. plików spakowanych oraz skompresowanych,
12. dysków sieciowych,
13. dysków przenośnych.
14. Rozwiązanie posiada opcję umieszczenia na liście wykluczeń ze skanowania :
15. wybranych plików,
16. wybranych procesów,
17. wybranych lokalizacji,

1. wybranych rozszerzeń,
2. nazwy wykrycia,
3. sumy kontrolnej (SHA1).
4. Rozwiązanie posiada możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
5. Moduł HIPS posiada możliwość pracy w jednym z pięciu trybów:
6. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
7. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
8. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
9. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program samoczynnie przełącza się w tryb pracy oparty na regułach,
10. tryb inteligentny, w którym rozwiązanie powiadamia wyłącznie o szczególnie
11. podejrzanych zdarzeniach.
12. Rozwiązanie jest wyposażone we wbudowaną funkcję, która generuje pełny raport na temat stacji.
13. Funkcja, generująca taki log, posiada przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

14. Istnieje możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

1. Raport posiada :
2. Listę zainstalowanych aplikacji,
3. Listę usług systemowych,
4. Informacje o systemie operacyjnym i sprzęcie,
5. Listę aktywnych procesów i połączeń sieciowych,
6. harmonogram systemu operacyjnego,
7. Szczegóły pliku hosts,
8. Informacje o sterownikach.
9. Rozwiązanie posiada tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają następujące funkcje systemu
10. antywirus,
11. zapora osobista
12. sandbox,
13. antyspyware,
14. metody heurystyczne.
15. Rozwiązanie skanuje system wirtualny w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie posiada funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie zapewnia blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o :

1. typ urządzenia:
2. pamięci masowe,
3. optyczne pamięci masowe,
4. pamięci masowe Firewire,
5. urządzenia do tworzenia obrazów,
6. drukarki USB,
7. urządzenia Bluetooth,
8. czytniki kart inteligentnych,
9. modemy,
10. porty LPT/COM,
11. urządzenia przenośne.
12. parametry urządzenia:
13. numer seryjny,
14. producent,
15. model.
16. typ dostępu:
17. brak możliwości zapisu,
18. pełen dostęp,

1. ostrzeżenie użytkownika,
2. brak dostępu.
3. Rozwiązanie automatyczne wykrywa usługi zainstalowane na serwerze i tworzy dla nich odpowiednie wyjątki dla następujących usług:
4. MS SQL,
5. Active Directory,
6. IIS,
7. Sysvol,

8. DNS,
9. DHCP,
10. Hyper-V,
11. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
12. Rozwiązanie posiada wbudowany system IDS, który posiada następujące funkcjonalności:
13. Ochrona przed anomaliami sieciowymi, w tym :
14. Skanowanie portów TCP oraz UDP,
15. Wykrywanie duplikacji adresu IP,
16. Atak zatruwania ARP,
17. Nieprawidłowa długość pakietu TCP oraz UDP.
18. Ochrona przed atakami typu brute-force dla usług oraz protokołów:

1. RDP,
2. SMB,
3. My SQL,
4. MS SQL.
5. Możliwość dodawania wyjątków dla systemu IDS, w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
6. Rozwiązanie posiada moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
7. Zapora osobista działa w oparciu o reguły i posiada 60 wbudowanych reguł, stworzonych przez producenta.
8. Zapora osobista posiada cztery tryby pracy:
9. tryb automatyczny -- rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
10. tryb interaktywny -- rozwiązanie pyta się o każde nowo nawiązywane połączenie,
11. tryb oparty na regułach -- rozwiązanie blokuje ruch przychodzący i wychodzący,
12. tryb uczenia się -- rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator posiada możliwość skonfigurowania czasu działania trybu.

Ochrona serwera - Linux

1. Rozwiązanie wspiera systemy w tym :
2. RedHat Enterprise Linux (RHEL),
3. Rocky Linux,

1. Ubuntu,
2. Debian,
3. SUSE Linux Enterprise Server (SLES),
4. Oracle Linux,
5. Amazon Linux.
6. Rozwiązanie zapewnia wykrywanie i usuwanie zagrożeń typu:
7. wirus,
8. trojan,
9. robak,
10. adware,
11. spyware,
12. dialer,
13. phishing,
14. backdoor.
15. Rozwiązanie zapewnia możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
16. Rozwiązanie posiada wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy

sztucznej inteligencji. Istnieje możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie -- z użyciem jednej lub obu metod jednocześnie.

1. Rozwiązanie wspiera automatyczną, inkrementacyjną aktualizację silnika detekcji.
2. Rozwiązanie posiada możliwość wykluczania ze skanowania procesów.
3. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia :
4. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
5. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
6. Rozwiązanie zapewnia skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem :
7. całego dysku,
8. wybranych katalogów,
9. pojedynczych plików,
10. plików spakowanych oraz skompresowanych,
11. dysków sieciowych,
12. dysków przenośnych.
13. Rozwiązanie posiada opcję umieszczenia na liście wykluczeń ze skanowania :
14. wybranych plików,
15. wybranych procesów,
16. wybranych lokalizacji,
17. wybranych rozszerzeń.

1. Rozwiązanie pozwala na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie wymaga do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, w pełni wspiera rozwiązanie Dell EMC Isilon.
4. Rozwiązanie działa w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta zapewnia podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikroserwisu.
5. Rozwiązanie wykrywa oraz podejrzane działania w kontenerach i blokuje je. Ochrona skanuje kontener w następujących fazach:
6. proces budowania obrazu kontenera,
7. wdrażanie obrazu kontenera.

Ochrona maszyn wirtualnych wdrożonych w środowiskach chmury publicznej Microsoft Azure, Amazon Web Services i/lub Google Cloud Platform.

1. Konsola centralnego zarządzania dostępna w wersji chmurowej posiada możliwość zarządzania i ochrony maszyn wirtualnych wdrożonych w chmurach publicznych.
2. Rozwiązanie do ochrony maszyn wirtualnych pochodzi od tego samego producenta.
    1. Wspierane środowiska chmurowe: Microsoft Azure,
    2. Amazon Web Services,
    3. Google Cloud Platform.
    4.
    5. Wspierane systemy maszyn wirtualnych:

        1. Windows,
        2. Linux.
        3.

1. Rozwiązanie pozwala na włączenie i wyłączenie funkcji automatycznej ochrony nowych i istniejących maszyn wirtualnych.

Mobile Device Management (MDM)

1. Konsola centralnego zarządzania dostępna w wersji chmurowej posiada możliwość zarządzania urządzeniami mobilnymi -- MDM.
2. MDM pochodzi od tego samego producenta konsoli centralnego zarządzania.
3. MDM umożliwia zarządzanie urządzeniami mobilnymi z systemami:
4. Android,
5. iOS,
6. iPadOS.
7. MDM posiada możliwość integracji z następującymi rozwiązaniami:
8. Microsoft Entra ID (w zakresie synchronizacji użytkowników),
9. Microsoft Intune (w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
10. VMware Workspace One (w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
11. Apple Business Manager (ABM),
12. Android Enterprise (w zakresie Device Owner).
13. MDM zapewnia wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

1. usunięcie zawartości urządzenia,
2. przywrócenie urządzenia do ustawień fabrycznych,
3. zablokowanie urządzenia,
4. uruchomienie sygnału dźwiękowego,
5. lokalizację GPS,
6. Resetowanie hasła blokady ekranu.
7. MDM zapewnia administratorowi podejrzenie listy zainstalowanych aplikacji.
8. MDM umożliwia :
9. Dla systemów iOS oraz iPadOS
10. konfigurację kont e-mail,
11. konfigurację połączeń VPN,
12. Konfigurację połączeń Wi-Fi,
13. Konfigurację listy certyfikatów,
14. możliwość uruchomienia trybu jednej aplikacji.
15. Dla systemu Android:
16. blokadę wykonywania połączeń,
17. blokadę konfiguracji sieci Wi-Fi,
18. blokadę konfiguracji tuneli VPN,

1. zarządzenie aktualizacjami sytemu operacyjnego,
2. blokadę zmiany tapety urządzenia.

Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie posiada pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie zapewnia 2 poziomy skanowania:
3. Inteligentne -- tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
4. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
5. Rozwiązanie zapewnia automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
6. Rozwiązanie posiada możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

7. Złożoność kodu blokady ekranu:
8. Wzór,
9. PIN,
10. Hasło,
11. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
12. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
13. Rozwiązanie posiada blokowanie aplikacji w oparciu o:
14. nazwę aplikacji,

1. nazwę pakietu,
2. kategorię sklepu Google Play,
3. uprawnienia aplikacji,
4. pochodzenie aplikacji z nieznanego źródła.
5. Rozwiązanie posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie jest integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie pochodzi od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie wspiera systemy w tym :
4. Microsoft Windows 10 oraz 11,
5. Microsoft Windows Server,
6. macOS 11 (Big Sur) oraz nowszych
7. RedHat Enterprise Linux (RHEL),
8. Rocky Linux,
9. Ubuntu,
10. Debian,
11. SUSE Linux Enterprise Server (SLES),

1. Oracle Linux,
2. Amazon Linux.
3. Rozwiązanie zapewnia ochronę przed zagrożeniami 0-day.
4. Rozwiązanie wykorzystuje do działania chmurę producenta tego samego rozwiązania antywirusowego.
5. Rozwiązanie posiada możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym :
6. archiwa,
7. skrypty,
8. pliki wykonywalne,
9. pliki rejestru systemowego (.reg),
10. możliwy spam,
11. dokumenty.
12. Administrator ma możliwość zdefiniowania po jakim czasie przesłane pliki zostają usunięte z
13. serwerów producenta w tym :
14. natychmiast po ich przeanalizowaniu,
15. po upływie 30 dni,
16. nigdy.
17. Administrator ma możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
18. Rozwiązanie pozwala na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

1. Administrator ma możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzania.
2. Rozwiązanie pozwala na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
3. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
4. Administrator ma dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
5. Przeanalizowane pliki zostają odpowiednio oznaczone. Analiza pliku kończy się jednym z poniższych wyników:
6. czysty,
7. podejrzany,
8. bardzo podejrzany,
9. szkodliwy.
10. W przypadku stacji roboczych rozwiązanie posiada możliwość wstrzymania uruchamiania pobieranych plików z następujących źródeł:
11. przeglądarki internetowe,
12. programy poczty e-mail,
13. nośniki wymienne,
14. pliki wyodrębnione z archiwum.
15. W przypadku serwerów pocztowych rozwiązanie posiada możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
16. Wykryte zagrożenia zostają przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

Szyfrowanie

1. Rozwiązanie pochodzi od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie bazuje na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie wspiera systemy operacyjne Windows (Windows 10/Windows 11).
4. Rozwiązanie umożliwia zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie posiada autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
6. Rozwiązanie umożliwia całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
7. Uwierzytelnienie użytkownika odbywa się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
8. W przypadku gdy użytkownik zapomni hasła, administrator ma możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania:
9. Hasło odzyskiwania po użyciu zostaje zmodyfikowane.
10. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
11. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
12. Rozwiązanie umożliwia szyfrowanie danych tylko na komputerach z UEFI.
13. Rozwiązanie umożliwia zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
14. Rozwiązanie umożliwia wykorzystanie modułu TPM w wersji 2.0.

1. Rozwiązanie wspiera dyski wykorzystującego funkcji OPAL w wersji 2.0.
2. W przypadku awarii urządzenia, administrator ma możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR pochodzi od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR jest realizowana przy pomocy dedykowanego konektora, który pochodzi od tego samego producenta rozwiązania antywirusowego.

3. Rozwiązanie zbiera następujące informacje z systemu operacyjnego:
4. tworzenie procesów,
5. uruchamianie, zatrzymanie i modyfikacja usług,
6. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,
7. usuwanie oraz zmiana nazw plików,
8. tworzenie i usuwanie kluczy rejestru systemowego,
9. ładowanie bibliotek DLL,
10. zalogowanie użytkowników,
11. elementy sieciowe, w tym:
12. pobranie plików wykonywalnych,
13. zestawienie połączeń TCP/IP,
14. zapytania HTTP,

1. zapytania DNS.
2. Rozwiązanie posiada ponad 1500 wbudowanych reguł, po których wystąpieniu, następuje wyzwolenie alarmu bezpieczeństwa.
3. Administrator ma możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania
4. automatyzacji tych reguł, opartych na następujących akcjach:
5. blokowanie pliku wykonywalnego,
6. blokowanie pliku wykonywalnego i poddanie go kwarantannie,
7. blokowanie podejrzanej biblioteki DLL,
8. zakończenie procesu,
9. skanowanie komputera w poszukiwaniu zagrożeń,
10. wyłączenie komputera,
11. izolacja sieciowa hosta,
12. wylogowanie użytkownika,
13. Administrator posiada możliwość utworzenia własnych reguł w oparciu o język XML.
14. Rozwiązanie posiada możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
15. Utworzenie wykluczenia automatycznie rozwiązuje alarmy historyczne, które pasują do utworzonego wykluczenia.
16. Podstawowe wykluczenia są konfigurowane w oparciu o przynajmniej: proces,
17. proces nadrzędny (proces rodzica),
18. nazwę procesu,

1. ścieżkę procesu,
2. wiersz polecenia,
3. wydawcę,
4. typ podpisu,
5. SHA-1,
6. SHA-2,
7. użytkownika.
8. Administrator ma możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
9. Rozwiązanie ma możliwość blokowania plików po sumach kontrolnych.
10. W ramach blokady istnieje możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
11. Blokowanie pliku jest możliwe na podstawie następujących funkcji skrótu (funkcje hashujące):
12. SHA-1,
13. SHA-256.
14. Rozwiązanie daje możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
15. hash pliku SHA-1,

16. hash pliku SHA-256,
17. hash pliku MD5,
18. typ sygnatury podpisu cyfrowego,

1. wydawcę certyfikatu,
2. wersję pliku,
3. oryginalną nazwę pliku,
4. rozmiar pliku,
5. reputację i popularność pliku w oparciu o system reputacji producenta tego samego
6. rozwiązania antywirusowego,
7. pierwsze uruchomienie pliku w środowisku,
8. ostatnie uruchomienie pliku w środowisku.
9. Rozwiązanie daje możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
10. oznaczania ich jako bezpieczne lub niebezpieczne,
11. pobierania ich do dalszej analizy, a pobierany plik jest zabezpieczony hasłem,
12. zablokowania wykonywania i wykorzystania pliku,
13. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
14. Rozwiązanie daje możliwość weryfikacji uruchomionych skryptów w środowisku wraz z

informacją dotyczącą parametrów uruchomienia (wiersz poleceń).

1. Administrator posiada możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
2. pobierania ich do dalszej analizy, a pobierany plik jest zabezpieczony hasłem.
3. Rozwiązanie posiada możliwość mapowania wykrycia na techniki, taktyki i procedury opisane w MITRE ATT&CK.

1. Rozwiązanie umożliwia graficzną wizualizacje zdarzeń wykrytych na stacjach roboczych.
2. Wizualizacja zawiera :
3. szczegóły wykrytego zdarzenia,
4. procesy, które uruchomiły dane wykrycie,
5. procesy potomne,
6. działania sieciowe podejrzanego procesu,
7. szczegóły pliku wykonywalnego, który uruchomił proces,
8. działania na plikach,
9. modyfikacje rejestru systemowego,
10. listę użytkowników.
11. Rozwiązanie pozwala na izolację hosta od sieci.
12. Administrator ma dostęp do funkcjonalności, która pozwala pobrać pliki z hosta do celów

dochodzeniowych.

1. Pobrane pliki są automatycznie zabezpieczone hasłem.
2. Administrator ma możliwość uruchomienia komendy wiersza poleceń na zdalnym hoście.
3. Rozwiązanie wspiera pracę z następującymi terminalami:
4. PowerShell oraz Windows Command Prompt dla systemu Windows,
5. Rozwiązanie posiada możliwość aktualizacji konektora EDR z poziomu konsoli centralnego zarządzania.

1. Administrator posiada możliwość blokady wybranego pliku po jego sumie kontrolnej.
2. Administrator ma możliwość szybkiego dodawania wyjątków z poziomu szczegółów wykrycia, dla następujących wartości:
3. nazwa procesu,
4. pełna ścieżka do procesu,

5. wiersz poleceń,
6. procesu rodzica,
7. SHA-1.

Ochrona serwera Microsoft Exchange

1. Rozwiązanie pochodzi od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie wspiera serwery pocztowe Microsoft Exchange w wersjach:
3. Exchange Server 2010 SP3,
4. Exchange Server 2013,
5. Exchange Server 2016,
6. Exchange Server 2019.
7. Rozwiązanie posiada możliwość skanowania poczty przychodzącej, wychodzącej oraz

wewnętrznej.

1. Rozwiązanie umożliwia administratorowi definiowanie reguł ochrony poczty w oparciu o:

1. nadawcy,
2. odbiorcy,
3. wielkość załącznika,
4. datę,
5. nagłówka wiadomości,
6. wynik SPF, DKIM i DMARC.
7. Rozwiązanie umożliwia wysłanie komunikatu do nadawcy lub odbiorcy z informacją o wykrytym zagrożeniu.
8. Komunikat jest możliwy do dostosowania przez administratora.
9. W przypadku wykrycia zagrożenia, rozwiązanie może wykonać następujące akcje:
10. usunięcie zainfekowanego załącznika i dostarczenie treści wiadomości,
11. usunięcie całej wiadomości,
12. przeniesienie wiadomości do dedykowanej kwarantanny.
13. Rozwiązanie posiada dedykowaną kwarantannę, która jest dostępna z poziomu przeglądarki internetowej.
14. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia :
15. Konfigurację wysyłania plików do analizy.
16. Konfigurację dodatkowych wykluczeń rozszerzeń i rodzajów plików, które nie mają być wysyłane do analizy.
17. Rozwiązanie posiada możliwość wysyłania próbek do analizy sandboxowej, po wykryciu

podejrzanych załączników.

1. Administrator ma możliwość konfiguracji, aby urządzenie końcowe oczekiwało z otworzeniem
2. załącznika do momentu zakończenia analizy sandbox.

Ochrona Microsoft 365

1. Rozwiązanie pochodzi od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie wspiera ochronę następujących usług Microsoft 365:
3. Exchange Online,
4. SharePoint Online,
5. OneDrive,
6. Microsoft Teams.
7. Rozwiązanie umożliwia skanowanie plików w czasie rzeczywistym w następujących usługach:
8. SharePoint Online,
9. OneDrive.
10. Rozwiązanie umożliwia skanowanie wiadomości email oraz ich załączników przed ich

dostarczeniem.

1. Rozwiązanie posiada system wczesnego ostrzegania oparty na chmurze pochodzący od tego

samego producenta oprogramowania antywirusowego, który umożliwia :

1. Konfigurację wysyłania plików do analizy.
2. Konfigurację rodzajów plików, które nie mają być wysyłane do analizy.
3. W przypadku wykrycia zagrożenia w wiadomości e-mail, rozwiązanie może wykonać

następujące akcje:

1. usunięcie zainfekowanego załącznika i dostarczenie treści wiadomości,
2. usunięcie całej wiadomości,
3. przeniesienie wiadomości do folderu elementy usunięte,
4. przeniesienie wiadomości do folderu wiadomości-śmieci.
5. Rozwiązanie umożliwia skonfigurowanie polityk w oparciu o grupy Microsoft Entra ID.
6. Rozwiązanie posiada możliwość wysyłania próbek do analizy sandboxowej, po wykryciu podejrzanych załączników.
7. Rozwiązanie umożliwia wykluczanie skrzynek pocztowych ze skanowania.

Ochrona Google Workspace

1. Rozwiązanie pochodzi od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie wspiera ochronę następujących usług Google Workspace:
3. Gmail,

1. Google Drive (w tym Google Drive udostępnione).
2. Rozwiązanie umożliwia skanowanie plików w czasie rzeczywistym w następujących usługach:
3. Google Drive (w tym Google Drive udostępnione).
4. Rozwiązanie umożliwia skanowanie wiadomości email oraz ich załączników przed ich dostarczeniem.
5. W przypadku wykrycia zagrożenia w wiadomości e-mail, rozwiązanie może wykonać

następujące akcje:

1. usunięcie zainfekowanego załącznika i dostarczenie treści wiadomości,
2. usunięcie całej wiadomości,
3. przeniesienie wiadomości do folderu elementy usunięte,
4. przeniesienie wiadomości do folderu spam.
5. Rozwiązanie umożliwia wykluczanie skrzynek pocztowych ze skanowania.

Vulnerability and Patch Management

1. Rozwiązanie jest dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
2. Rozwiązanie ma możliwości wykrywania podatności:
3. w tym co najmniej następujących systemach operacyjnych:

➢ Windows,
➢ macOS,
➢ Linux

1. w aplikacjach zainstalowanych na zarządzanych stacjach.
2. Rozwiązanie posiada bazę podatności zawierającą co najmniej 35000 CVE.
3. Rozwiązanie nie wymaga instalacji dodatkowej konsoli ani innych dodatkowych

komponentów na stacjach końcowych. Zarządzanie musi się odbywać z poziomu tej samej konsoli co rozwiązanie antywirusowe, pochodzące od tego samego producenta.

1. Rozwiązanie umożliwia utworzenie haromonogramu automatycznego wykrywania

podatności.

1. Rozwiązanie umożliwia wyświetlanie szczegółów danej podatności zawierające co

najmniej:
1. nazwę aplikacji lub systemu operacyjnego
2. punktacje CVSS
3. opis wykrytej podatności
4. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
5. Rozwiązanie wykrywa podatności w 700 aplikacjach.
6. Rozwiązanie umożliwia wykonanie automatycznej aktualizacji dla 300 popularnych aplikacji.
7. Rozwiązanie umożliwia stworzenie białej listy aplikacji podlegających automatycznej aktualizacji:
8. Automatyczne aktualizacje będą aplikowane tylko dla wskazanych aplikacji w białej liście.

1. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
2. Rozwiązanie umożliwia stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji.
3. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich – ponad 300 aplikacji, oprócz aplikacji wskazanych na czarnej liście.
4. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
5. Rozwiązanie umożliwia ręczne wdrażanie poprawek na wybranych stacjach.
6. Rozwiązanie jest zintegrowane bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
7. Rozwiązanie umożliwia wyłączenie powiadomień dla wybranej podatności.

Two-factor authentication / multi-factor authentication
1. Rozwiązanie jest dostępne w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie umożliwia dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie jest zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie pozwala na instalację oprogramowania na co najmniej następujących systemach operacyjnych:

A. Systemy serwerowe:
1. Microsoft Windows Server 2012 R2,
2. Microsoft Windows Server 2016,
3. Microsoft Windows Server 2019,
4. Microsoft Windows Server 2022,

1. Microsoft Windows Server 2025.

B. Systemy kliencie:
1. Windows 10,
2. Windows 11.
3. Rozwiązanie posiada integrację z następującymi rozwiązaniami:
4. Microsoft Exchange,
5. Microsoft Dynamics CRM,
6. Microsoft Sharepoint,
7. Microsoft Remote Desktop Web Access,
8. Microsoft Terminal Services Web Access,
9. Microsoft Remote Web Access,
10. Active Directory Federation Services.
11. Rozwiązanie posiada wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników podczas logowania do co najmniej:
12. klienta VPN,
13. systemu macOS
14. systemu Linux,

15. połączenia SSH.
16. Rozwiązanie oferuje dedykowaną bezpłatną aplikację mobilną pochodzącą od tego samego producenta rozwiązania 2FA/MFA.

1. Aplikacja mobilna wspiera następujące systemy:
2. Android,
3. iOS.
4. Aplikacja mobilna umożliwia uwierzytelnienie użytkownika przy pomocy co najmniej:
5. Generowanego kodu OTP w tym co najmniej HOTP i TOTP.
6. Powiadomienia PUSH.
7. Aplikacja mobilna posiada możliwość zabezpieczenia jej przy pomocy kodu PIN oraz danych biometrycznych.
8. Aplikacja do działania nie wymaga od użytkownika aktywnego połączenia z Internetem – generowanie OTP odbywa się w trybie offline.
9. Aplikacja umożliwia generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.
10. Rozwiązanie oferuje alternatywne możliwości uwierzytelnienie użytkownika w tym:
11. OTP dostarczonego przy pomocy wiadomości SMS,
12. OTP dostarczonego przy pomocy wiadomości e-mail,
13. tokenu sprzętowego,
14. FIDO,
15. klucza odzyskiwania (MRK).

3 . Zarządzalne urządzenia sieciowe wraz z z usługą segmentacji sieci IT oraz konfiguracji systemów.

Element	Ilość	Wymagany zakres
Punkt dostępowy Wi-Fi 6	3	Dwupasmowy punkt dostępowy 802.11ax, klasa min. AX1800 (574 Mb/s + 1201 Mb/s), min. 4 strumienie; 1× RJ45 1 Gb/s; zasilanie PoE 802.3af/at; OFDMA, MU-MIMO, WPA3; min. 8 SSID, VLAN 802.1Q na SSID; roaming i mesh zarządzane z kontrolera; komplet uchwytów montażowych.
Switch 24-portowy PoE+	3	24× RJ45 10/100/1000 Mb/s PoE+ 802.3af/at, min. 30 W/port; PoE min. 250 W; 4× SFP 1 Gb/s; rack 19″; VLAN 802.1Q, STP/RSTP/MSTP, LACP, QoS, ACL, DHCP Snooping, IGMP Snooping, routing statyczny; zarządzanie z centralnego kontrolera; urządzenie fabrycznie nowe, z pełną gwarancją i wsparciem aktualizacji.
Switch 5-portowy PoE+	8	5× RJ45 10/100/1000 Mb/s, w tym min. 4× PoE+ 802.3af/at; budżet PoE min. 65 W; VLAN 802.1Q, QoS, izolacja portów, IGMP Snooping, ochrona przed pętlami i PoE Auto Recovery; centralne zarządzanie; konstrukcja bezwentylatorowa.
Kontroler sieciowy	1	Sprzętowy kontroler lokalny i chmurowy; obsługa co najmniej 15 AP i 7 switchy; min. 2 porty Ethernet, USB do kopii konfiguracji; zasilanie PoE 802.3af/at lub USB; zarządzanie przez WWW i aplikację; brak obowiązkowej subskrypcji; aktualna wersja dostępna w oficjalnej dystrybucji.
Szafa RACK	2	RACK 19″, 6U, głębokość montażowa min. 400 mm; kolor czarny; zamykane drzwi szklane; otwierane lub zdejmowane boki; min. 2 szyny montażowe; nośność min. 20 kg; komplet elementów montażowych.

Patchpanel kat. 5e STP	2	19″, 1U, 24 porty RJ45, kat. 5e, ekranowany STP, złącza IDC/LSA, oznaczenia portów i punkt uziemiający. Ekranowanie należy połączyć z prawidłowo uziemioną szafą; uziemienie instalacji nie jest objęte zamówieniem.
UPS	2	Zasilacz awaryjny UPS wolnostojący, topologia line-interactive, moc minimum 700 VA / 360 W, napięcie wejściowe i wyjściowe 230 V AC, automatyczna regulacja napięcia AVR, minimum 2 gniazda wyjściowe Schuko, przewód zasilający z wtykiem Schuko, czas przełączenia nie dłuższy niż 10 ms, akumulator kwasowo-ołowiowy lub równoważny, czas ładowania nie dłuższy niż 8 godzin, sygnalizacja LED i alarm dźwiękowy, ochrona przepięciowa minimum 273 J
Patchcord 0,5 m	48	Fabrycznie zakończony RJ45-RJ45, długość 0,5 m, kat. min. 5e, przepustowość 1 Gb/s, żyły miedziane, zalewane wtyki z ochroną zatrzasku, jeden kolor dla całej partii.
Półka stała RACK	4	Stała, perforowana, stalowa, 19″, wysokość 2U, głębokość min. 350 mm, kolor czarny, udźwig min. 25 kg; komplet śrub i nakrętek klatkowych.
Listwa zasilająca RACK	1	RACK 19″, min. 9 gniazd 230 V typu E/Schuko, wyłącznik, przewód min. 1,8 m, obciążalność min. 16 A, ochrona przeciwprzepięciowa lub zabezpieczenie nadprądowe; wtyk zgodny z gniazdami UPS.
Instalacja, montaż, konfiguracja i uruchomienie	1 usługa	Dostawa i dojazd, wniesienie, złożenie szafy stojącej, montaż szaf i wyposażenia RACK, montaż urządzeń oraz punktów dostępowych w przygotowanych miejscach, połączenia patchcordami, uruchomienie zasilania i kontrola PoE. Aktualizacja stabilnego firmware, adopcja urządzeń do kontrolera, konfiguracja portów access/trunk, przypisanie wskazanych VLAN do portów i sieci Wi-Fi, utworzenie SSID, ustawienia WPA2/WPA3, roamingu, izolacji gości i podstawowego monitoringu. Przekazanie kopii konfiguracji, zestawienia urządzeń i adresów zarządzających, tabeli portów/VLAN/SSID oraz protokołu wykonania i testów. W ramach realizacji zamówienia Wykonawca zobowiązany jest do dostawy niezbędnych materiałów oraz wykonania, zabezpieczenia, podłączenia i uruchomienia nowej linii sieciowych LAN, niezbędnych do uruchomienia nowych serwerów obejmującego: 1. Wykonanie **dwóch niezależnych linii sieciowych LAN** pomiędzy urządzeniem bezpieczeństwa UTM a pomieszczeniem serwerowni, z wykorzystaniem przewodów miedzianych kategorii minimum 6, o długości każdej linii nieprzekraczającej 50 m. 2. Wykonanie niezbędnego nowego okablowania LAN wewnątrz pomieszczenia serwerowni, umożliwiającego prawidłowe podłączenie i komunikację urządzeń serwerowych, sieciowych oraz pozostałej infrastruktury objętej zamówieniem. 3. Łączna długość nowo wykonanego okablowania LAN, obejmującego dwie linie pomiędzy urządzeniem UTM a serwerownią oraz pozostałe przewody wykonywane w serwerowni, nie przekroczy **300 metrów bieżących**. Szczegółowy przebieg tras kablowych oraz

		rozmieszczenie punktów połączeniowych zostaną uzgodnione z Zamawiającym przed rozpoczęciem prac. 4. Wykonanie niezbędnych tras kablowych, obejmujących prowadzenie przewodów w korytach instalacyjnych, listwach ochronnych, rurach osłonowych lub peszlach, odpowiednio do warunków technicznych pomieszczeń. Przewody należy zabezpieczyć przed uszkodzeniami mechanicznymi oraz ułożyć w sposób uporządkowany, zapewniający możliwość późniejszej konserwacji i rozbudowy instalacji. 5. Wykonanie niezbędnych przejść instalacyjnych przez ściany i przegrody budowlane oraz ich prawidłowe zabezpieczenie i wykończenie, z zachowaniem wymaganych zabezpieczeń przeciwpożarowych. 6. Zakończenie przewodów odpowiednimi złączami lub modułami RJ45 kategorii minimum 6, podłączenie do urządzenia UTM, przełączników sieciowych, patchpaneli oraz pozostałych urządzeń zgodnie z uzgodnioną konfiguracją. 7. Uporządkowanie i oznaczenie wykonanych połączeń sieciowych w serwerowni oraz zapewnienie odpowiedniego prowadzenia i zabezpieczenia przewodów w szafach RACK. 8. Przeprowadzenie testów i pomiarów poprawności wykonanych linii LAN, weryfikację ciągłości przewodów, prawidłowości połączeń oraz funkcjonowania transmisji danych. 9. Przekazanie Zamawiającemu dokumentacji powykonawczej, obejmującej wykaz wykonanych połączeń, oznaczenia przewodów, przebieg tras kablowych oraz wyniki przeprowadzonych testów. **Wszystkie materiały, przewody, elementy montażowe, zabezpieczenia, złącza oraz czynności niezbędne do wykonania i uruchomienia wskazanej infrastruktury LAN muszą być uwzględnione w cenie oferty Wykonawcy.**

4. Macierz dyskowa wraz z dyskami

Parametr	Minimalne wymagania techniczne
Typ urządzenia	Macierz dyskowa przeznaczona do pracy ciągłej w środowisku serwerowym.
Obudowa	Obudowa do montażu w szafie RACK 19”, wysokość maksymalnie 2U.
Liczba zatok dyskowych	Minimum 12 zatok dyskowych na dyski 3,5” SATA HDD, z możliwością obsługi dysków 2,5” SATA SSD/HDD przy zastosowaniu odpowiednich ramek lub adapterów.

Wymiana dysków	Zatoki dyskowe typu hot-swap / hot-plug, umożliwiające wymianę dysku bez wyłączania urządzenia, przy zachowaniu zasad właściwych dla skonfigurowanej macierzy RAID.
Procesor	Procesor 64-bitowy klasy serwerowej lub embedded, architektura x86-64 / x64, minimum 4 rdzenie / 8 wątków, taktowanie bazowe minimum 3,0 GHz lub procesor równoważny wydajnościowo.
Pamięć RAM	Minimum 8 GB RAM ECC, z możliwością rozbudowy do minimum 32 GB.
Dyski twarde	Minimum 12 szt. dysków twardych HDD klasy NAS lub enterprise, każdy o pojemności minimum 8 TB, format 3,5", interfejs SATA III 6 Gb/s, prędkość obrotowa minimum 7200 obr./min, przeznaczonych do pracy ciągłej 24/7 w środowisku RAID.
Łączna pojemność surowa	Minimum 96 TB brutto/surowo, liczona jako 12 × 8 TB.
Pamięć cache dysków	Minimum 256 MB pamięci cache na każdy dysk lub parametr równoważny właściwy dla dysków klasy NAS/enterprise.
Kompatybilność dysków	Dyski muszą być w pełni kompatybilne z oferowaną macierzą, znajdować się na liście kompatybilności producenta oferowanego urządzenia lub być formalnie dopuszczone do pracy w tym urządzeniu. Niedopuszczalne jest zaoferowanie dysków powodujących ograniczenie funkcjonalności, ostrzeżenia o niekompatybilności, brak możliwości aktualizacji oprogramowania dysków albo utratę wsparcia producenta macierzy.
RAID	Obsługa co najmniej RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10. Wymagana możliwość skonfigurowania macierzy odpornej na awarię minimum jednego dysku oraz konfiguracji odpornej na awarię minimum dwóch dysków.
Rekomendowana konfiguracja	Macierz powinna zostać skonfigurowana w trybie zapewniającym odporność na awarię co najmniej dwóch dysków, np. RAID 6 lub równoważnym, chyba że Zamawiający na etapie wdrożenia zdecyduje inaczej.
System plików	Obsługa systemu plików zapewniającego integralność danych, migawki lub mechanizmy ochrony przed przypadkową zmianą/usunięciem danych.
Migawki danych	Możliwość tworzenia migawek udziałów lub wolumenów oraz przywracania danych z migawek.
Protokoły plikowe	Obsługa co najmniej SMB/CIFS, NFS, FTP/SFTP lub równoważnych mechanizmów udostępniania zasobów plikowych.
Obsługa iSCSI	Obsługa iSCSI Target/LUN, z możliwością tworzenia zasobów blokowych dla serwerów lub środowisk wirtualizacyjnych.
Interfejsy sieciowe	Minimum 2 × RJ-45 1GbE oraz minimum 1 × RJ-45 10GbE, wbudowany lub dostarczony jako karta rozszerzeń, gotowy do pracy w oferowanej konfiguracji.
Agregacja łączy	Obsługa agregacji portów sieciowych, w tym co najmniej IEEE 802.3ad / LACP, jeżeli infrastruktura Zamawiającego będzie to wspierać.
Porty zewnętrzne	Minimum 2 porty USB 3.0 / USB 3.2 Gen 1 lub równoważne.
Rozbudowa	Minimum jeden slot rozszerzeń umożliwiający instalację dodatkowej karty sieciowej, karty rozszerzeń lub innego modułu przewidzianego przez producenta urządzenia.
Zasilanie	Minimum 2 redundantne zasilacze hot-swap, pracujące w układzie nadmiarowym. Awaria jednego zasilacza nie może powodować wyłączenia urządzenia.
Chłodzenie	Chłodzenie wielowentylatorowe z monitorowaniem stanu wentylatorów i temperatury.

Zarządzanie	Wbudowany system zarządzania dostępny przez przeglądarkę internetową, umożliwiający zarządzanie dyskami, wolumenami, udziałami, użytkownikami, uprawnieniami, usługami sieciowymi, aktualizacjami, alertami oraz raportami stanu urządzenia.
Kontrola dostępu	Obsługa kont lokalnych oraz integracji z usługą katalogową, w szczególności z domeną opartą o usługę katalogową. Wymagane zarządzanie uprawnieniami użytkowników i grup do udziałów sieciowych.
Monitorowanie	Monitorowanie stanu dysków, wolumenów, macierzy RAID, temperatury, wentylatorów, zasilaczy, obciążenia procesora, użycia pamięci RAM, wykorzystania przestrzeni dyskowej oraz interfejsów sieciowych.
Powiadomienia i alerty	Możliwość wysyłania powiadomień o błędach, awariach dysków, degradacji macierzy, przekroczeniu temperatury, problemach z zasilaniem oraz błędach usług.
Logi systemowe	Prowadzenie dzienników zdarzeń administracyjnych i systemowych oraz możliwość ich przeglądu, eksportu lub przekazywania do zewnętrznego systemu logowania.
Bezpieczeństwo administracyjne	Obsługa kont administracyjnych, haseł, ról/uprawnień, dziennika logowań oraz mechanizmu podnoszącego bezpieczeństwo logowania administracyjnego, np. uwierzytelniania wieloskładnikowego, jeżeli oferowane rozwiązanie go wspiera.
Diagnostyka lokalna	Wskaźniki LED lub równoważny system sygnalizacji informujący o stanie zasilania, pracy systemu, błędach, aktywności sieci oraz stanie dysków.
Diagnostyka zdalna	Możliwość zdalnej diagnostyki przez panel administracyjny, w tym podgląd stanu urządzenia, dysków, wolumenów, macierzy, temperatury, zasilaczy, wentylatorów i usług.
Osprzęt	Komplet szyn montażowych RACK, przewody zasilające, ramki/kieszenie dyskowe, dokumentacja oraz wszystkie elementy niezbędne do montażu i uruchomienia.
	Gwarancja Serwer z co najmniej 24 miesięczną gwarancją, świadczona na miejscu u klienta z czasem reakcji serwisu w miejscu instalacji maksymalnie do 3 godzin roboczych w godzinach pracy Zamawiającego tj.: Poniedziałek - Piątek: 7:00 - 15:00. Serwisowe zgłoszenia za pomocą kodów QR. W ramach tej funkcji użytkownicy mają możliwość zgłaszać serwisowe problemy, skanując kod QR umieszczony na obudowie serwera. Po zeskanowaniu kodu zostaną przekierowani do formularza zlecenia serwisowego z wypełnionym automatycznie numerem seryjnym serwera, bez konieczności instalacji dodatkowych aplikacji. Formularz musi być zintegrowany systemem informatycznym Wykonawcy, w celu automatycznego stworzenia zlecenia serwisowego na podstawie wypełnionych danych w formularzu.

5 . System bezpieczeństwa UTM wraz z oprogramowaniem

Wymagane minimalne parametry techniczne
Ilość 1 szt.

Wymagania Ogólne

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.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

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.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 5 portami Gigabit Ethernet RJ-45.

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.

3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1 Gbps.

6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

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.

4. Ochrona przed malware.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. 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.

10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.

12. 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: adresy 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. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec 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).

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. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

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 usłudze chmurowej realizowanej na terenie Unii Europejskiej.

8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

9. 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. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).

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. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.

6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

7. 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. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. 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.

3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

9. 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 (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.

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 wieloskładnikowego 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.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

Serwisy i licencje

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

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 36 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz

CZĘŚĆ 2 – OPIS PRZEDMIOTU ZAMÓWIENIA

Poniżej znajduje się opis przedmiotu zamówienia dla Części 2.

OPIS PRZEDMIOTU ZAMÓWIENIA – CZĘŚĆ 2

Projekt: „Cyberbezpieczne Wodociągi”

Zamawiający: Miasto i Gmina Solec nad Wisłą

Załącznik do SWZ – opis przedmiotu zamówienia dla Części 2 postępowania prowadzonego zgodnie z ustawą Prawo zamówień publicznych.

I. Nazwa i zakres Części 2

Część 2: dostawa, wdrożenie, konfiguracja i utrzymanie zintegrowanego zakresu organizacyjno-kompetencyjnego oraz programowego służącego podniesieniu poziomu cyberbezpieczeństwa Zamawiającego.

Część 2 obejmuje łącznie trzy zadania, które powinny być realizowane jako spójny zakres odpowiedzialności Wykonawcy:

- Zadanie 2.1 – opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) oraz wdrożenie, przegląd, aktualizacja oraz zarządzanie i doskonalenie, zakończone audytem SZCD ; doradztwo w zakresie opracow. warunków umów kontraktowych na wdrożenie z usługami wspomagającymi realizację projektu.
- Zadanie 2.2 – szkolenia z zakresu cyberbezpieczeństwa dla kadry oraz pracowników wraz z testami socjotechnicznymi.
- Zadanie 2.3 – dostawa, wdrożenie, konfiguracja, integracja i utrzymanie zintegrowanego środowiska oprogramowania cyberbezpieczeństwa obejmującego backup, menadżera logów/SIEM, funkcjonalność XDR, ochronę poczty, DLP oraz środowisko wirtualizacyjne.

Niniejszy dokument dotyczy wyłącznie Części 2 postępowania i stanowi kompletny opis przedmiotu zamówienia dla tej części.

II. Kody CPV

Kod CPV	Nazwa CPV	Zastosowanie w Części 2
48730000-4	Pakiety oprogramowania zabezpieczającego	oprogramowanie bezpieczeństwa, funkcje SIEM/XDR, DLP, ochrona poczty
48710000-8	Pakiety oprogramowania do kopii zapasowych i odzyskiwania	backup, odtwarzanie danych, retencja
48732000-8	Pakiety oprogramowania do zabezpieczania danych	ochrona danych, DLP, zabezpieczenia dostępu
72268000-1	Usługi dostawy oprogramowania	dostarczenie lub udostępnienie komponentów oprogramowania
72263000-6	Usługi wdrażania oprogramowania	wdrożenie komponentów systemowych
72265000-0	Usługi konfiguracji oprogramowania	konfiguracja polityk, reguł, integracji, alertów i raportów
72250000-2	Usługi w zakresie konserwacji i wsparcia systemów	utrzymanie i wsparcie do 31 grudnia 2026 r.
72611000-6	Usługi w zakresie wsparcia technicznego	zdalne wsparcie, konsultacje, obsługa zgłoszeń
80500000-9	Usługi szkoleniowe	szkolenia z zakresu cyberbezpieczeństwa

79212000-3	Usługi audytu	audytowe kompetencje zespołu przy opracowaniu dokumentacji i zgodności

III. Cel zamówienia

- podniesienie poziomu bezpieczeństwa teleinformatycznego i organizacyjnego Zamawiającego;
- opracowanie dokumentacji ciągłości działania i odtwarzania po awarii zgodnej z wymaganiami projektu oraz dobrymi praktykami PN-EN ISO/IEC 27001 i PN-EN ISO 22301;
- przeprowadzenie audytu wdrożonego SZCD;
- doradztwo i usługi wspomagające realizację projektu oraz wsparcie w rozliczeniu projektu;
- zwiększenie świadomości kadry i pracowników w zakresie cyberbezpieczeństwa, w tym poprzez testy socjotechniczne;
- zapewnienie centralnego monitorowania i analizy zdarzeń bezpieczeństwa;
- wdrożenie mechanizmów wykonywania i odtwarzania kopii zapasowych;
- ograniczenie ryzyka ataków pocztowych, nieuprawnionego dostępu, utraty danych i wycieku informacji;
- zapewnienie środowiska wirtualizacyjnego dla komponentów bezpieczeństwa;
- zapewnienie bieżącego wsparcia wdrożeniowego i utrzymaniowego do dnia 31 grudnia 2026 r.

IV. Wymagania ogólne dla Części 2

- Wykonawca odpowiada za spójność merytoryczną, techniczną i organizacyjną wszystkich zadań objętych Częścią 2.
- Opis przedmiotu zamówienia został sformułowany funkcjonalnie i jakościowo. Zamawiający nie wskazuje nazw producentów, znaków towarowych, modeli ani konkretnych nazw handlowych oprogramowania.
- Nazwy klas rozwiązań, takie jak SIEM, XDR, DLP, backup, Email Secure Gateway lub wirtualizacja, należy rozumieć jako określenia kategorii funkcjonalnych.
- Wykonawca może zaoferować rozwiązania komercyjne, otwartoźródłowe lub mieszane, pod warunkiem zapewnienia legalności korzystania, kompletności kosztów, wsparcia oraz odpowiedzialności za prawidłowe wdrożenie.
- Wszystkie koszty niezbędne do wykonania zamówienia, w tym licencje, subskrypcje, wdrożenie, konfiguracja, integracja, dokumentacja, instruktaż, utrzymanie i wsparcie do 31 grudnia 2026 r., muszą być ujęte w cenie oferty.
- Wykonawca zobowiązany jest zachować poufność wszystkich informacji uzyskanych w związku z realizacją zamówienia.

V. Zadanie 2.1 – dokumentacja SZCD, wdrożenie, audyt SZCD

1. Przedmiot zadania

Przedmiotem zadania jest opracowanie i przekazanie dokumentacji Systemu Zarządzania Ciągłością Działania (SZCD) i odtwarzania po awarii (DRP), wdrożenie, przegląd, aktualizacja oraz zarządzanie i doskonalenie, zakończone audytem SZCD. Dokumentacja zgodna z PN-EN ISO 22301 oraz powiązanych z wymaganiami bezpieczeństwa informacji, dla systemów informatycznych IT oraz systemów sterowania OT Zamawiającego.

2. Zakres dokumentacji

Grupa dokumentów	Minimalny zakres
Dokumenty SZCD – 8 szt.	polityka ciągłości działania, analiza BIA, analiza ryzyka, struktura i role, obsługa incydentów i kryzysów, utrzymanie i testowanie, wskaźniki KPI, monitorowanie ryzyka
Plany BCP i DRP – 6 szt.	plan BCP, plan DRP, plan odtworzenia OT, plan komunikacji kryzysowej, plan testów, raport z testu
Karty procesów i systemów	do 8 kart procesów krytycznych oraz do 12 kart systemów krytycznych IT/OT łącznie

Warsztaty	do 6 spotkań po 4 godziny, łącznie do 24 godzin, zdalnie lub stacjonarnie, zgodnie z ustaleniami z Zamawiającym
Korekty	jedna runda uwag zgłaszana zbiorczo przez Zamawiającego

3. Zasady realizacji dokumentacji

- Prace prowadzone są dokumentacyjnie i warsztatowo, bez obowiązku dostępu do środowisk produkcyjnych, chyba że Strony uzgodnią inaczej.
- Podstawą opracowania są informacje, materiały i dokumenty przekazane przez Zamawiającego, w szczególności wykazy systemów, procedury, umowy, informacje o procesach oraz wymagania organizacyjne.
- Parametry ciągłości działania, w tym MTPD/MAO, RTO i RPO, ustala się na podstawie danych Zamawiającego.
- Dokumentacja zostanie przekazana w formie edytowalnej .docx i/lub .xlsx oraz dodatkowo w PDF, jeżeli Zamawiający tego wymaga.
- Odbiór nastąpi na podstawie protokołu oraz wykazu przekazanych plików.

4. Współprca z Zamawiającym, terminy

- Wyznaczenie koordynatora oraz właścicieli procesów : do 3 dni od zawarcia umowy.
- Przekazanie dokumentacji istniejącej (umowy, procedury, wykazy systemów): do 7 dni.
- Udział wskazanych osób w warsztatach: w terminach uzgodnionych.
- Zatwierdzenie wykazu procesów i systemów krytycznych: do 14 dni od przekazania.
- Zgłoszenie uwag do dokumentów (zbiorczo, jednorazowo): do 5 dni roboczych.
- Zatwierdzenie dokumentacji: do 7 dni od przekazania.

5. Audyt SZCD

- Przeprowadzony po przygotowaniu dokumentacji SZCD oraz zakończeniu wdrożenia.
- Prowadzony przez audytora posiadającego certfikat audytora wiodącego wg normy ISO/IEC 22301.
- Audyt zakończony raportem ze wskazaniem kierunków doskonalenia.
- Audyt w formacie pdf, podpisany podpisem elektronicznym.

6. Doradztwo i usługi wspomagające realizację projektu

- Doradztwo w zakresie opracow. warunków umów kontraktowych na wdrożenie i utrzymanie infrastruktury w zakresie cyberbezpieczeństwa.
- Usługi wspomagające realizację projektu.
- Wsparcie w przygotowaniu dokumentacji konkursowej, doradztwo w spełnieniu warunków konkursowych oraz rozliczenie projektu do 31.XII.2026r.

VI. Zadanie 2.2 – szkolenia i testy socjotechniczne

1. Przedmiot zadania

Przedmiotem zadania jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry i pracowników Zamawiającego oraz przeprowadzenie działań powiązanych z testami socjotechnicznymi weryfikującymi świadomość zagrożeń i reakcje personelu.

2. Minimalny program szkolenia dla kadry

- podstawy prawne bezpieczeństwa informacji, w tym KSC, NIS2 i ochrona danych;
- polityka bezpieczeństwa informacji – cel, zakres i główne zasady;
- system zarządzania bezpieczeństwem informacji, role i odpowiedzialności;
- ochrona informacji w organizacji, klasyfikacja informacji i dostęp do zasobów;
- incydenty bezpieczeństwa i ogólne zasady zgłaszania;
- podsumowanie, pytania i odpowiedzi.

3. Minimalny program szkolenia dla pracowników

- znaczenie cyberbezpieczeństwa dla podmiotu publicznego;
- obowiązki wynikające z przepisów prawa i zasad wewnętrznych;
- zagrożenia: ataki socjotechniczne, phishing, spear phishing, spoofing, vishing, smishing, ransomware, DDoS, deepfake;
- zasady bezpiecznej pracy z pocztą elektroniczną i Internetem;
- konsekwencje utraty danych;
- praca zdalna;
- zasady korzystania z Internetu oraz poczty e-mail:
- bezpieczeństwo pracy zdalnej, 2FA, szyfrowanie, ochrona urządzeń służbowych;
- kopie zapasowe, konsekwencje utraty danych, objawy zainfekowanego komputera;
- podstawowe czynności obsługi i zgłaszania incydentów.

4. Testy socjotechniczne

- kontrolowane wiadomości phishingowe, np. fałszywe powiadomienia od kuriera, banku, urzędu lub dostawcy usługi;
- testowe scenariusze vishingu, jeżeli Zamawiający dopuści taką formę testu;
- testowe wiadomości SMS lub inne symulacje smishingu, jeżeli Zamawiający dopuści taką formę testu;
- omówienie wyników testów, wskazanie najskuteczniejszych scenariuszy i obszarów ryzyka

5. Warunki organizacyjne szkoleń

- 2 dni szkoleniowe, łącznie dla maksymalnie 32 osób;
- 4 szkolenia, przy czym czas jednego szkolenia wynosi do 5 godzin szkoleniowych po 45 minut;
- tryb stacjonarny, chyba że Zamawiający dopuści tryb zdalny lub hybrydowy;
- w siedzibie Zamawiającego;
- szkolenie w dni robocze, w trakcie godzin pracy urzędu;
- materiały informacyjne dla uczestników w formie broszury, publikacji lub materiału elektronicznego;
- zaświadczenia o ukończeniu szkolenia, lista obecności oraz dokumentacja odbiorowa.

VII. Zadanie 2.3 – zintegrowane środowisko oprogramowania cyberbezpieczeństwa

1. Model wdrożenia zdalnego i instalacji przez GPO

Zamawiający wymaga, aby wdrożenie komponentów programowych było realizowane zdalnie z wykorzystaniem bezpiecznego dostępu administracyjnego oraz mechanizmów centralnej dystrybucji oprogramowania w domenie Zamawiającego.

- Instalacja komponentów końcowych, agentów, konfiguracji lub skryptów na stacjach roboczych i serwerach dołączonych do domeny musi odbywać się wyłącznie przez mechanizmy GPO.
- Wykonawca nie będzie zobowiązany ani uprawniony do osobistej instalacji komponentów na pojedynczych stanowiskach pracy, chyba że Zamawiający pisemnie zleci czynności dodatkowe.
- Wykonawca przygotuje pakiety instalacyjne, skrypty, parametry uruchomieniowe, polityki lub instrukcje niezbędne do dystrybucji oprogramowania przez GPO.
- Wykonawca uzgodni z Zamawiającym zakres jednostek organizacyjnych, grup zabezpieczeń, harmonogram wdrożenia, grupę pilotażową, sposób weryfikacji skuteczności instalacji oraz procedurę wycofania zmian.
- Przed wdrożeniem produkcyjnym Wykonawca przeprowadzi pilotaż na uzgodnionej grupie urządzeń.
- Komponenty centralne, serwerowe lub administracyjne, których nie dystrybuuje się przez GPO, zostaną zainstalowane lub skonfigurowane zdalnie z wykorzystaniem bezpiecznego dostępu administracyjnego.
- Po zakończeniu wdrożenia Wykonawca przekaże dokumentację zastosowanych GPO, zakres objętych urządzeń, wyniki weryfikacji instalacji oraz zalecenia powdrożeniowe.

2. Wymagania ogólne dla oprogramowania

- Rozwiązanie musi być gotowe do użytkowania produkcyjnego po odbiorze końcowym.
- Rozwiązanie musi umożliwiać zarządzanie przez uprawnionych administratorów Zamawiającego.
- Rozwiązanie musi zapewniać kontrolę dostępu administracyjnego, rozdzielenie ról lub uprawnień, o ile dany komponent posiada taką funkcję.
- Rozwiązanie musi rejestrować działania administracyjne i zdarzenia istotne z punktu widzenia bezpieczeństwa.
- Rozwiązanie musi umożliwiać wykonywanie kopii konfiguracji wdrożonych komponentów.
- Rozwiązanie musi umożliwiać generowanie raportów technicznych i bezpieczeństwa.
- Rozwiązanie musi umożliwiać aktualizację komponentów, reguł, sygnatur, polityk, wzorców detekcji lub innych mechanizmów bezpieczeństwa.
- Rozwiązanie musi być opisane w dokumentacji powdrożeniowej w sposób pozwalający Zamawiającemu na dalsze utrzymanie środowiska.

3. Oprogramowanie do wykonywania kopii zapasowych, w tym deduplikacji

- wykonywanie kopii zapasowych danych, konfiguracji, maszyn wirtualnych lub wybranych zasobów systemowych wskazanych przez Zamawiającego;
- obsługa harmonogramów zadań backupu oraz możliwość ręcznego uruchamiania kopii;
- obsługa kopii pełnych oraz przyrostowych lub różnicowych, jeżeli pozwala na to wdrożone rozwiązanie;
- mechanizmy deduplikacji, kompresji albo inne mechanizmy ograniczające powielanie danych;
- definiowanie retencji kopii zapasowych i zasad usuwania starszych kopii;
- raportowanie statusu wykonania zadań i powiadamianie administratora o błędach;
- rejestrowanie zdarzeń dotyczących backupu, odtwarzania i zmian konfiguracji;
- zabezpieczenie dostępu administracyjnego do systemu backupu;
- możliwość wykonania testu odtworzeniowego po wdrożeniu oraz ujęcie wyniku w protokole testów;
- przygotowanie procedury wykonywania, monitorowania i odtwarzania kopii zapasowych, obejmującej harmonogram, retencję, zakres backupu i tryb postępowania w przypadku nieudanego zadania.

4. Menadżer logów / SIEM oraz monitorowanie zdarzeń bezpieczeństwa

- centralne gromadzenie logów z systemów operacyjnych, serwerów, usług sieciowych, urządzeń sieciowych, poczty i komponentów bezpieczeństwa, o ile umożliwia to środowisko Zamawiającego;

- obsługa standardowych mechanizmów przesyłania logów, w szczególności agentów, syslog, plików dzienników lub interfejsów API, jeżeli są dostępne;
- normalizacja, porządkowanie, indeksowanie i wyszukiwanie zdarzeń;
- wyszukiwanie zdarzeń według czasu, źródła, typu zdarzenia, poziomu istotności, użytkownika, hosta lub innego dostępnego parametru;
- tworzenie reguł detekcji, alertów bezpieczeństwa i paneli administracyjnych;
- korelacja zdarzeń pozwalająca identyfikować potencjalne incydenty;
- raportowanie okresowe i incydentalne, w tym eksport raportów do plików;
- przechowywanie logów przez okres uzgodniony z Zamawiającym, z uwzględnieniem dostępnej przestrzeni dyskowej;
- prowadzenie dziennika czynności administracyjnych;
- wykrywanie i raportowanie zdarzeń dotyczących nieudanych logowań, podejrzanej aktywności kont, zmian konfiguracji, błędów systemowych i anomalii możliwych do zidentyfikowania na podstawie dostępnych logów.

5. Funkcjonalność klasy XDR

Przez funkcjonalność klasy XDR Zamawiający rozumie mechanizm rozszerzonego wykrywania i analizy zagrożeń wykorzystujący dane z wielu źródeł. Rozwiązanie nie musi być oznaczone handlowo jako XDR, jeżeli spełnia poniższe wymagania funkcjonalne.

- zbieranie informacji o zdarzeniach z chronionych systemów końcowych, serwerów, logów, usług sieciowych, poczty lub innych źródeł dostępnych w środowisku Zamawiającego;
- analiza zdarzeń pod kątem zagrożeń bezpieczeństwa i klasyfikacja alertów według poziomu istotności;
- wykrywanie podejrzanych zachowań użytkowników, procesów lub usług;
- wykrywanie prób nieautoryzowanego dostępu, eskalacji uprawnień, zmian w konfiguracji bezpieczeństwa lub naruszeń integralności wybranych plików;
- możliwość definiowania i modyfikowania reguł, polityk lub scenariuszy detekcji;
- obsługa incydentu przez administratora, w tym możliwość odnotowania statusu, komentarza lub podjętych działań;
- integracja z centralnym systemem logowania i raportowania;
- generowanie raportów bezpieczeństwa dotyczących zdarzeń, alertów i trendów.

6. Ochrona poczty elektronicznej

- analiza wiadomości przychodzących oraz, jeżeli architektura Zamawiającego umożliwia takie wdrożenie, wiadomości wychodzących;
- filtrowanie spamu, phishingu, wiadomości podszywających się pod nadawcę oraz wiadomości z podejrzanymi lub złośliwymi załącznikami;
- obsługa kwarantanny wiadomości i możliwość ich przeglądu, zwalniania lub usuwania przez administratora;
- definiowanie polityk filtrowania, list dozwolonych i blokowanych nadawców oraz reguł wyjątków;
- raportowanie zdarzeń pocztowych oraz przekazywanie logów do centralnego systemu monitorowania, jeżeli jest to technicznie możliwe;
- konfiguracja lub weryfikacja mechanizmów ograniczających podszywanie się pod domenę Zamawiającego, w szczególności SPF, DKIM i DMARC, o ile Zamawiający dysponuje wymaganym dostępem do DNS i systemu pocztowego;
- prace ingerujące w produkcyjny przepływ poczty muszą być uzgadniane z Zamawiającym z wyprzedzeniem i realizowane w sposób minimalizujący ryzyko przerwy.

7. Mechanizmy przeciwdziałania wyciekowi danych – DLP

- identyfikacja, ewidencjonowanie i raportowanie danych wrażliwych lub chronionych oraz ryzyk związanych z ich przechowywaniem i dostępem;
- definiowanie wzorców wyszukiwania danych, w tym danych osobowych, identyfikacyjnych, finansowych lub innych kategorii wskazanych przez Zamawiającego;
- skanowanie wybranych zasobów plikowych, systemowych lub sieciowych udostępnionych przez Zamawiającego;
- wskazanie lokalizacji danych wymagających dodatkowego zabezpieczenia;
- oznaczanie ryzyk związanych z nadmiernym lub nieuprawnionym dostępem do danych;

- formułowanie rekomendacji działań ograniczających ryzyko wycieku;
- dokumentowanie wyników analizy oraz raportowanie wyników do Zamawiającego;
- jeżeli rozwiązanie posiada funkcje ostrzegania, blokowania lub wymuszania polityk, Wykonawca skonfiguruje je w zakresie uzgodnionym z Zamawiającym.

8. Środowisko wirtualizacyjne dla systemów bezpieczeństwa

- tworzenie i uruchamianie maszyn wirtualnych lub równoważnych środowisk izolowanych;
- zarządzanie zasobami procesora, pamięci, dysków i sieci;
- uruchomienie komponentów związanych z backupem, analizą logów, ochroną poczty, DLP, XDR lub innymi systemami bezpieczeństwa;
- ograniczenie dostępu administracyjnego i rejestrowanie zdarzeń administracyjnych;
- tworzenie kopii konfiguracji środowiska;
- możliwość wykonywania kopii lub migawek maszyn wirtualnych, jeżeli jest to technicznie uzasadnione i bezpieczne dla danego komponentu;
- konfiguracja sieci wirtualnej z uwzględnieniem separacji usług bezpieczeństwa od pozostałych elementów infrastruktury, o ile pozwala na to środowisko Zamawiającego;
- przekazanie dokumentacji konfiguracji środowiska.

9. Integracja komponentów

- przekazywanie logów z systemu ochrony poczty do centralnego systemu logów, jeżeli jest to technicznie możliwe;
- przekazywanie logów z systemu backupu i środowiska wirtualizacyjnego do centralnego systemu logów;
- konfiguracja alertów dotyczących zdarzeń bezpieczeństwa;
- konfiguracja raportów okresowych;
- uzgodnienie z Zamawiającym podstawowych scenariuszy reakcji na alerty;
- weryfikacja poprawności działania integracji;
- wykonanie testów działania wdrożonego środowiska.

VIII. Harmonogram, dokumentacja, testy i odbiór

Etap	Nazwa etapu	Zakres	Rezultat
1	Analiza przedwdrożeniowa	Przegląd środowiska Zamawiającego, zakresu dokumentacji, źródeł logów, backupu, poczty, DLP, szkoleń i GPO.	Raport lub nota z analizy.
2	Projekt techniczny i harmonogram	Uzgodnienie kolejności prac, warsztatów, okien serwisowych, zakresu testów i pilotażu GPO.	Harmonogram i założenia konfiguracyjne.
3	Realizacja dokumentacji i szkoleń	Opracowanie dokumentacji SZCD/BCP/DRP, przeprowadzenie szkoleń i testów socjotechnicznych.	Dokumentacja, listy obecności, zaświadczenia, raport z testów.
4	Instalacja i konfiguracja oprogramowania	Zdalne uruchomienie komponentów centralnych; instalacja komponentów końcowych przez GPO; konfiguracja polityk, reguł, kont, retencji, alertów i raportów.	Działające środowisko, dokumentacja GPO, protokół testów.
5	Testy i poprawki	Testy backupu, odtwarzania, logów, alertów, poczty, DLP, wirtualizacji, GPO i integracji.	Raport z testów.
6	Dokumentacja i instruktaż	Przekazanie dokumentacji powdrożeniowej i instruktaż administratorów.	Dokumentacja i potwierdzenie instruktażu.

7	Odbiór końcowy	Podpisanie protokołu odbioru po spełnieniu wymagań OPZ.	Protokół odbioru końcowego.
8	Wsparcie i utrzymanie	Wsparcie techniczne i utrzymaniowe do 31 grudnia 2026 r.	Ewidencja zgłoszeń i raport końcowy wsparcia.

IX. Dokumentacja powdrożeniowa i odbiorowa

- opis architektury wdrożonego środowiska;
- wykaz wdrożonych komponentów, wersji, ról systemowych i zależności;
- opis konfiguracji systemu backupu, retencji i procedury odtwarzania;
- opis konfiguracji menadżera logów/SIEM, źródeł logów i reguł detekcji;
- opis konfiguracji funkcjonalności XDR oraz alertów;
- opis konfiguracji ochrony poczty elektronicznej;
- opis konfiguracji mechanizmów DLP;
- opis konfiguracji środowiska wirtualizacyjnego;
- opis zastosowanych GPO, zakres objętych urządzeń i wyniki weryfikacji instalacji;
- wykaz skonfigurowanych kont administracyjnych lub ról, bez ujawniania haseł;
- procedury backupu, obsługi alertów i zgłaszania problemów;
- raport z testów i zalecenia powdrożeniowe;
- dokumentacja szkoleniowa, listy obecności, zaświadczenia oraz raport z testów socjotechnicznych;
- dokumentacja SZCD, BCP i DRP z rejestrem wydania;
- odbiór raportu z audytu.

Hasła, klucze dostępowe i inne dane poufne nie mogą być wpisywane bezpośrednio do dokumentacji ogólnej. Powinny zostać przekazane Zamawiającemu odrębnym, uzgodnionym i bezpiecznym kanałem.

X. Testy odbiorowe

- wykonanie testowej kopii zapasowej oraz testowego odtworzenia danych lub konfiguracji;
- sprawdzenie odbioru logów z wybranych źródeł;
- sprawdzenie działania alertów bezpieczeństwa i raportów;
- sprawdzenie działania ochrony poczty elektronicznej;
- sprawdzenie działania mechanizmów wykrywania ryzyk DLP;
- sprawdzenie dostępu administracyjnego i uprawnień;
- sprawdzenie działania środowiska wirtualizacyjnego;
- sprawdzenie działania dystrybucji przez GPO na grupie pilotażowej lub testowej;
- sprawdzenie poprawności integracji komponentów;
- sprawdzenie kompletności dokumentacji szkoleniowej.

Pozytywny wynik testów jest warunkiem odbioru końcowego, chyba że Zamawiający zaakceptuje odbiór z zastrzeżeniami i terminem usunięcia usterek.

XI. Instruktaż administratorów

- podstawową obsługę wdrożonych systemów;
- analizę alertów i generowanie raportów;
- obsługę backupu i odtwarzania danych;
- obsługę kwarantanny poczty;
- interpretację wyników DLP;
- podstawową obsługę środowiska wirtualizacyjnego;
- zasady dystrybucji komponentów przez GPO i weryfikacji instalacji;
- zasady zgłaszania problemów w okresie wsparcia;

- zasady aktualizacji i utrzymania środowiska.

XII. Wsparcie techniczne i utrzymanie do 31 grudnia 2026 r.

Wykonawca zapewni wsparcie techniczne i utrzymaniowe dla wdrożonego środowiska do dnia 31 grudnia 2026 r. Wsparcie obejmuje wdrożone komponenty, ich konfigurację, integracje, dokumentację powdrożeniową, obsługę zgłoszeń oraz konsultacje dotyczące użytkowania rozwiązania.

- konsultacje techniczne dotyczące wdrożonego środowiska;
- pomoc w analizie alertów i zdarzeń bezpieczeństwa;
- pomoc w usuwaniu błędów konfiguracji;
- wsparcie w aktualizacji komponentów, reguł, polityk, harmonogramów i raportów;
- wsparcie w odtwarzaniu danych z kopii zapasowych;
- wsparcie w analizie problemów z przepływem poczty elektronicznej;
- wsparcie w interpretacji raportów DLP;
- wsparcie w utrzymaniu środowiska wirtualizacyjnego;
- przygotowywanie rekomendacji naprawczych i usprawniających;
- prowadzenie ewidencji zgłoszeń, zdalnych sesji wsparcia, wdrożeń przez GPO i wykonanych czynności;
- sporządzenie raportu końcowego po zakończeniu okresu wsparcia.

Priorytet	Opis	Czas reakcji
Krytyczne	Brak działania kluczowego komponentu lub ryzyko istotnego zakłócenia pracy środowiska bezpieczeństwa.	do 2 godzin roboczych
Wysokie	Istotne ograniczenie funkcjonalności, brak części integracji, problem z raportowaniem lub alertami.	do 8 godzin roboczych
Standardowe	Konsultacje, zmiany konfiguracyjne, modyfikacje raportów, wyjaśnienia i rekomendacje.	do 2 dni roboczych
Niskie	Pytania organizacyjne, drobne korekty dokumentacji, sugestie usprawnień.	do 3 dni roboczych

XIII. Warunki uczestnictwa / warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się Wykonawcy, których zespół realizujący zadania objęte Częścią 2 będzie dysponował łącznie następującymi osobami i kompetencjami składającymi się z:

- co najmniej 1 osoby posiadającej kwalifikacje audytora wiodącego wg normy ISO/IEC 27001 co najmniej od 3 lat oraz kwalifikacje audytora wiodącego wg normy ISO/IEC 22301 co najmniej od 3 lat, z doświadczeniem obejmującym co najmniej 10 wdrożeń, opracowań, audytów lub prac dotyczących SZBI z elementem ciągłości działania na rzecz podmiotów publicznych, wykonanych w ciągu ostatnich 3 lat;

- co najmniej 1 szkoleniowca posiadającego kwalifikacje audytora wiodącego wg normy ISO/IEC 27001 oraz wg normy ISO/IEC 22301, z doświadczeniem w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa od co najmniej 3 lat, który przeprowadził co najmniej 10 szkoleń o tematyce cyberbezpieczeństwa na rzecz podmiotów publicznych.

Dopuszcza się dysponowanie osobami na podstawie umowy o pracę, umowy cywilnoprawnej, współpracy B2B, zobowiązania podmiotu trzeciego lub innej podstawy prawnej zapewniającej realną dostępność tych osób w okresie realizacji zamówienia.

Dokumenty wymagane na potwierdzenie warunków uczestnictwa

Dokument	Zakres potwierdzenia
Certyfikat / dokument kwalifikacji audytora wiodącego ISO/IEC 27001	potwierdzenie kwalifikacji audytorskich osoby wskazanej do realizacji zamówienia
Certyfikat / dokument kwalifikacji audytora wiodącego ISO/IEC 22301	potwierdzenie kwalifikacji audytorskich w obszarze ciągłości działania
Wykaz prac audytora / eksperta	co najmniej 5 prac/projektów SZBI z elementem ciągłości działania na rzecz podmiotów publicznych w ostatnich 3 latach
Wykaz szkoleń szkoleniowca	co najmniej 10 szkoleń z cyberbezpieczeństwa na rzecz podmiotów publicznych oraz doświadczenie szkoleniowe od co najmniej 3 lat
Wykaz osób skierowanych do realizacji zamówienia	funkcja, zakres czynności, doświadczenie, kwalifikacje i podstawa dysponowania
Oświadczenie Wykonawcy	potwierdzenie dysponowania zespołem oraz gotowości do przedłożenia dokumentów przed zawarciem umowy, jeżeli Zamawiający tego zażąda
Zobowiązanie podmiotu trzeciego / podwykonawcy / osoby	w przypadku korzystania z zasobów podmiotów trzecich lub podwykonawców – potwierdzenie realnej dostępności zasobów

Wykonawca przekaże stosowne dokumenty potwierdzające wymagane kwalifikacje audytorskie oraz złoży oświadczenie wraz z wykazami przeprowadzonych prac przez audytora i szkoleniowca. Dokumenty składane są zgodnie z wymaganiami SWZ oraz w terminach określonych przez Zamawiającego.

XIV. Podwykonawstwo

- Zamawiający dopuszcza wykonywanie prac przez podwykonawców.
- Wykonawca wskaże w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, oraz poda nazwy podwykonawców, jeżeli są już znani.
- Powierzenie wykonania części zamówienia podwykonawcy nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.
- Osoby wskazane przez podwykonawców mogą potwierdzać spełnienie wymagań dotyczących potencjału osobowego, o ile Wykonawca wykaże realną dostępność tych osób na potrzeby realizacji zamówienia.
- Wykonawca odpowiada za zachowanie poufności przez podwykonawców oraz za bezpieczeństwo informacji przekazanych w związku z realizacją zamówienia.

XV. Podmiotowe i przedmiotowe środki dowodowe

Rodzaj dokumentu	Zakres
Karta zgodności z OPZ	potwierdzenie spełnienia każdego wymagania minimalnego i wskazanie sposobu jego spełnienia
Opis techniczny oferowanego rozwiązania	opis komponentów, architektury, integracji, modelu wsparcia, instalacji przez GPO i utrzymania
Oświadczenie o legalności oprogramowania	potwierdzenie legalności licencji, subskrypcji lub warunków korzystania z komponentów otwartoźródłowych
Opis sposobu wdrożenia zdalnego	opis narzędzi, dostępu, bezpieczeństwa, pilotażu GPO, procedury wycofania zmian i testów
Wykaz usług / prac i dowody należytego wykonania	potwierdzenie doświadczenia Wykonawcy i/lub osób skierowanych do realizacji zamówienia

Wykaz osób i dokumenty kwalifikacyjne	potwierdzenie kwalifikacji audytora, szkoleniowca i osób technicznych